CYBERSECURITY MINDFULNESS

CyberAtomics: Computational Thermodynamic Weapons of Mass Destruction – Malware Pretending to be Digital Assets.

January Walker [1]

[1] Cybersecurity Mindfulness 1; January.Walker@CybersecurityMindfulness.com

Abstract

I received a letter written by United States Senator Elizabeth Warren who implored the investigation the power draw and pollution that cryptocurrencies and specifically Bitcoin were having on the planet. The following Cyber Threat Report (CTR) is the public disclosure of my cybersecurity investigation. A special thanks to Jordan Gerton at the University of Utah for whiteboarding with me and providing crucial feedback at a critical moment during my investigation.

There is no cybersecurity risk greater than the risk to life itself. If there is no life, there is no threat to protect it from. At a glance Bitcoin appears to be a financial theory. In looking deeper it's a one-way entropy machine that threatens human health, environmental health, the bees, cybersecurity systems, financial systems, and now the nation itself with the Bitcoin reserve. This disclosure highlights real & time sensitive cybersecurity threats. As Bitcoin can emit the equivalent of 2,099,993.63 Hiroshima bombs I am classifying it as a CyberAtomic which must be shut down immediately.

Keywords: Physics; Information physics; Financial Theory; Entropy; Politics; Cryptocurrency; Bitcoin; Proof-of-Work; Cancer; Social Engineering; Cybersecurity Mindfulness; Whitehouse; Malware

Introduction

I write this for humanity and the continuation of the earth & life itself and to provide exact, reproducible methodology for calculating Bitcoin's Shannon entropy signature for forensic malware detection analysis. The target audience is cybersecurity professionals, investigators, policy makers, institutional security analysts, financial institutions, those in possession of the malware. Humanity deserves transparency.

1. Malware

Thermodynamic Weapons

A thermodynamic weapons framework operates on the principle that you don't need to destroy infrastructure directly. You embed high-entropy information processing into the same environment as critical infrastructure. The system does two things simultaneously: Generates continuous thermal and entropy load on the local environment. Creates dependency through economic, social, and technical integration. The infrastructure cannot function without the energy supply. The embedded system cannot function

Editor: January Walker

Received: January 20, 2026
Published: January 28, 2026

without consuming that energy through irreversible processes. The result is systematic degradation of available energy in the system—a ratchet that tightens over time This is distinct from traditional weapons that cause acute damage. This is a thermodynamic siege: the slow, irreversible conversion of available resources into entropy until the system cannot maintain itself.

A framework of power consumption analysis has emerged as a robust malware detection mechanism grounded in the fundamental principle that malware execution necessarily demands computational resources. Research from IEEE and Oak Ridge National Laboratory demonstrates that malware can be accurately detected via power data analytics, with anomaly detection systems achieving perfect detection rates when leveraging comprehensive feature sets across multiple task categories **[1]**. This approach exploits the fact that malicious processes cannot execute without consuming measurable power, creating a thermodynamic constraint that adversaries cannot circumvent.

Resource anomalies provide corroborating evidence of infection. Unusual spikes in CPU and memory utilization often indicate malware activity, with ransomware implementations notably generating sudden surges in processing demand as they encrypt file systems **[2]**. More specifically, forensic analysis standards establish that systems under normal idle conditions typically exhibit resource utilization below 10%, making elevated CPU usage during periods of expected inactivity a significant indicator of potential viral infection **[3]**.

Complementing power-based detection, entropy analysis provides a complementary forensic signature. Approximately 50% of malware samples exhibit entropy values of 7.2 or greater—a threshold strongly correlated with packing, encryption, and compression techniques that form standard components of malware development **[4]**. High-entropy blocks have become a hallmark of detection methodologies, particularly for identifying ransomware variants that rely on encryption as their primary obfuscation mechanism **[5]**. The prevalence of entropy-based signatures in modern malware detection reflects the consistent operational pattern of adversaries leveraging cryptographic techniques to evade traditional signature-based detection systems.

The cryptocurrency Bitcoin and its proponents state that bitcoin needs continuous access to power for entropy generation. How much entropy though is Bitcoin creating and how much energy is it using?

2. Malware Analysis with Shannon's Entropy

Shannon Entropy and Fair Coin Flip

Shannon entropy measures the average amount of information or uncertainty in a data set by calculating how predictable or random the distribution of symbols is **[6]**. The formula is defined as:

$$H(X) = -\Sigma\ P(x) \times \log_2(P(x))$$

Shannon entropy is important because it provides an objective, measurable way to distinguish between random/encrypted data and structured/unencrypted data **[7]** through entropy production. High entropy ($H \geq 7.2$) indicates encryption or compression, which is the forensic signature used to identify both malware and systems designed to obscure their operations **[8]**. Low entropy indicates structure and predictability. Shannon's entropy is defined by the following terms.

$H(X)$ = Shannon entropy (measured in bits)
$P(x)$ = probability of symbol x occurring
Σ = sum across all possible symbols
$\log_2$ = logarithm base 2

In order to begin the analysis, we start with a fair coin flip. A fair coin flip represents the highest level of uncertainty in a binary system because neither outcome is more likely than the other **[9]**—you have no way to predict whether it will be heads or tails.

For a fair coin where both outcomes are equally likely:

$$P(\text{heads}) = 0.50$$
$$P(\text{tails}) = 0.50$$

Expand the summation (Σ) for both outcomes:

$$H(X) = -\Sigma\, P(x) \times \log_2(P(x))$$
$$H = -[P(\text{heads}) \times \log_2(P(\text{heads})) + P(\text{tails}) \times \log_2(P(\text{tails}))]$$

We then follow the following set of instructions
1. Calculate the $\log_2(0.5)$
2. Plug in the probabilities
3. Plug in the log values
4. Multiply
5. Add inside brackets
6. Apply the negative sign

$$\log_2(0.5) = -1$$
$$H = -[0.5 \times \log_2(0.5) + 0.5 \times \log_2(0.5)]$$
$$H = -[0.5 \times (-1) + 0.5 \times (-1)]$$
$$H = -[-0.5 + -0.5]$$
$$H = -[-1]$$
$$H = 1 \text{ bit}$$

The Result is a fair coin flip has entropy of 1 bit—maximum entropy for a binary choice.

Maximum Entropy Principle
The Maximum Entropy Principle states that entropy reaches its highest value when all possible outcomes are equally likely **[6]**. If you have N possible symbols and they all appear with equal probability, then $P(x) = 1/N$ for each symbol.

Example 1: Fair coin (N = 2 possible outcomes)

$$P(\text{heads}) = 1/2 = 0.5$$
$$P(\text{tails}) = 1/2 = 0.5$$
$$H\_max = \log_2(2) = 1 \text{ bit}$$

Example 2: Fair die (N = 6 possible outcomes)

$$P(1) = P(2) = P(3) = P(4) = P(5) = P(6) = 1/6$$
$$H\_max = \log_2(6) = 2.585 \text{ bits}$$

Example 3: File byte (N = 256 possible values)

$$P(0) = P(1) = \ldots = P(255) = 1/256$$
$$H\_max = \log_2(256) = 8 \text{ bits}$$ **[6]**

When all symbols are equally likely, you get maximum uncertainty. You have no way to predict which symbol will appear next. This is why a file with all 256-byte values appearing equally has maximum entropy (8 bits per byte) **[6]**.

Step-by-step derivation
$P(x) = 1/N$ for all N symbols

$$H(X) = -\Sigma\, P(x) \times \log_2(P(x))$$
$$H = -[(1/N) \times \log_2(1/N) + (1/N) \times \log_2(1/N) + \ldots + (1/N) \times \log_2(1/N)]$$
$$H = -[N \times (1/N) \times \log_2(1/N)]$$
$$H = -[\log_2(1/N)]$$
$$H = -[-\log_2(N)]$$
$$H = \log_2(N)$$
$$H\_max = \log_2(N)$$

Verify with fair coin (N = 2)

$$H\_max = \log_2(N) = \log_2(2) = 1 \text{ bit} \checkmark$$

We may now perform an analysis on the byte and by leveraging the same equation.

$$H\_max = \log_2(256) = ?$$
$$2^8 = \log_2(256) = 8 \text{ bits}$$

For example, fully written out the number is quite large
115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936

A single byte has 256 possible values (0-255). When all are equally likely, the entropy is 8 bits. This is the maximum entropy per byte in computer files.

Another example is the SHA-256 Hash Output where we can use the Use logarithm property $\log_2(2^n) = n$

N possible states = 2^{256} =

$$H\_max = \log_2(2^{256}) = ?$$
$$H\_max = \log_2(2^{256}) = 256 \text{ bits}$$

The SHA-256 produces 256-bit outputs. When all 2^{256} possible hash values are equally likely (which they are by design), the maximum entropy is 256 bits **[10]**.

To normalize the bits to the 0 – 8 forensic scale used in malware analysis I calculate the entropy by (256 bits / 256 bits) × 8 = 8.0/8.0 **[8]**.

Table 1. Malware Entropy Benchmark

ENTROPY	INTERPRETATION
0.0	No entropy. Completely ordered, all bytes identical.
3.0 - 4.0	Typical uncompressed text/code.

5.0 - 6.0	Some compression/structure present.
7.0 - 7.2	Compressed or slightly encrypted data.
7.2 +	Malware Threshold, an encrypted, or packed suspicious.
8.0	Entropic Malware & maximum entropy.

Benchmark

Practical Security Analytics Benchmark is the Standard used by computer forensics industry. As all 2^{256} possible outputs are equally likely the maximum entropy is 256 bits **[8]**.

$$H\_max = \log_2(2^{256}) = 256 \text{ bits}$$

In benchmarking Bitcoins entropy at an 8.0/8.0, I obtain ≥ 7.2 by 0.8 points exceeding the malware detection threshold by 11% (0.8/7.2).

3. Malware or Software?

Forensic analysis distinguishes between user-controlled encryption tools and autonomous malicious processes based on operational control parameters and the Key forensic differentiator between malware an encryption is the off switch. For example, in apps like Signal, a user can disable, delete app, and stop using. In a Document a user may navigate to the menu and remove encryption. In malware there is no ability to given to the user to remove or control its persistence.

Malware persistence is defined as "the ability for the malware to survive a reboot of the system" and emphasize that persistence requires "the ability for an attacker to retain access for as long as possible" [9]. The key distinction is that malware operates against user intent—once deployed, it continues functioning independently of the user's wishes. MITRE ATT&CK framework defines persistence as techniques "that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code" [10].

Bitcoin is defined as a Decentralized Autonomous Organization, DAO [11] for short where the network. DAO have no user control and "acts autonomously and separately from its members and their wills and determinations" [14]. Critically, Bitcoin operates as a self-organizing system where "The network is fully self-organizing, and there is no governance model built" while the progress and adoption of ideas is slow" [12].

Further Bitcoin's decentralized structure "ensures redundancy, meaning that no single node is critical to the network's operation" and that "even if some nodes are shut down or restricted by local authorities, the network remains functional and beyond the direct control of any single national regulation authority" [13]. Creating a critical vulnerability to integrated infrastructures for cyberattacks.

Both malware and Bitcoin share the defining characteristic of operating continuously regardless of individual or collective user intent. Neither has an "off-switch" that users can activate. Both persist autonomously across system reboots/network disruptions. Both are resistant to centralized control or shutdown.

Bitcoin has no off switch, and for the most critical infrastructures—the energy grids. Operates 24/7/365 regardless of user desire

4. Bitcoin's Cryptography

Analyzing Bitcoin
To analyze the Bitcoin's Mining algorithm I identify its encryption [14][15]. Bitcoin uses the Secure Hash Algorithm 256-bit which has the following properties

1. Input: Any data of any length (transaction block headers, 80 bytes typical)

2. Output: 256 bits (32 bytes) fixed length

3. Output representation: 64 hexadecimal characters Design goal:

4. Cryptographically random output [14]

SHA-256 is a cryptographic hash function specified in NIST FIPS PUB 180-4 [14]. The algorithm processes input data of arbitrary length and produces a fixed 256-bit output, regardless of input size. This deterministic property means identical inputs always produce identical outputs, making the process reproducible and verifiable [14][15].

SHA-256 Randomness Characteristics
SHA-256 exhibits three critical properties relevant to entropy analysis.

Property 1: The Avalanche Effect
A single-bit change in input produces approximately 128 bits of change in output on average [14]. This avalanche property means the output cannot be predicted from minor input variations and appears unpatterned to statistical analysis.

Example:
Input: Bitcoin → Output: 8a4d9f3c2e1B7f5a...
Input: Bitcoin → Output: 6f2a1c7e4d9b3f8a...

Even if only 1 character changed like a capital B to lowercase b the hash is completely different from the first.

The outputs are completely different. You cannot see any relationship between them. If you only know the first hash (8a4d9f...), you cannot predict the second hash (6f2a1c...) even if you know the inputs differ by only one letter.

The outcome is you cannot reverse-engineer the input from the output or predict what the output will be without running the algorithm. The output behaves like random data, even though the process is completely deterministic [14]. Changing even one character produces an entirely different hash.

The avalanche property is why Bitcoin's mining requires continuous guessing: tiny changes to the input (like incrementing a nonce counter) produce completely unpredictable outputs. There is no pattern or shortcut—you must compute each hash individually [12].

Property 2: Deterministic Hashing
Deterministic hashing means the same input always produces the same output, without exception. The behavior is predictable and reproducible and not random in the probabilistic sense, resulting in the output itself exhibits maximum entropy [14]. Deterministic hashing is a requirement for blockchain systems—the entire network must agree on the hash value for any given block [14][15].

Input: block_header_A → Always produces hash_X
Input: block_header_A → Always produces hash_X (consistent)

Every time you hash the exact same block header; you get the exact same result. This consistency is absolute and verified across the entire Bitcoin network. If two nodes produce different hashes for the same block header, the blockchain fork is detected and resolved [15].

The implication of "deterministic" means the outcome is fixed and repeatable. It is not probabilistic randomness where outcomes vary each time. Instead, it is engineered pseudo-randomness—the output appears random and unpredictable, but the process itself is completely deterministic **[14]**.

The key distinction between probabilistic randomness and deterministic pseudo-randomness is in probabilistic randomness if you flip a coin 100 times you get different sequences each time. In deterministic pseudo-randomness you can hash the same input 100 times and get identical output every time, but that output appears random and unpredictable **[14]**.

This determinism is critical because the entire network can independently verify any hash is correct No randomness or luck is involved—only computational work The blockchain ledger is unchangeable: altering any past block changes its hash, which breaks the chain **[15]** The output behaves like random data (unpredictable, no patterns), but the process is perfectly reproducible **[14]**.

Property 3: A One-Way Function
A one-way function is a function that is easy to compute in one direction but computationally infeasible to reverse **[14]**. Meaning the original input cannot be recovered from the output. This asymmetry is fundamental to Bitcoin's functional architecture and means the output contains no recoverable structure from the input .

For example, within the byte framework you cannot reverse hash_X → original input given a hash output (hash_X). The one-way function is fundamental to Bitcoin's architecture **[15]**. If hashes were to be reversed, the entire blockchain would be compromised—anyone could forge transactions by working backwards from desired hash values. The only way to find an input that produces hash_X is to map inputs and hash them until you find a match **[14]**.

The one-way property ensures sequential hashing or brute force computation **[15]**.

5. Bitcoin Mining Entropy Generation Rate

Understanding Hashrate
A "hash" is one execution of the SHA-256 algorithm. Bitcoin miners compete by computing hashes continuously, trying to find a hash output that meets specific criteria

(starts with a certain number of zeros). The "hashrate" measures how many hashes the entire Bitcoin network computes per second [16][17]. The Bitcoin network performs approximately 950 quintillion hash computations every second.

To calculate the discarded bits

Entropy bits per second = Hashes per second × Bits per hash x Bits per hash: 256 bits (SHA-256 output)

Given the hash rate exceeded 950 EH/s by 2025 I calculate the following.

Hashrate = 950 EH/s
Hashrate = 950×10^{18} hashes/second
Hashrate = 9.5×10^{20} hashes/second

Hashrate = $9.5 \times 10^{20} \times 256$ hashes/second
Hashrate = 2.432×10^{23} bits per second
Hashrate = 243,200,000,000,000,000,000,000 bits per second (s)

For context 243 septillionths is more bits discarded per second than exist in all digital storage on Earth and comes with a thermodynamic cost regardless of storage.

To Scale the strain on critical infrastructure we calculate hour, day, and yearly hashrates.

Hashrate = 2.432×10^{23} bits/s × 3600 s = 8.755×10^{26} bits/hr.
Hashrate = 950×10^{18} bits/s × 86,400 s = 2.101×10^{28} bits/day
Hashrate = 9.5×10^{20} bits/s × 31,557,600 s = 7.674×10^{30} bits/year

Bitcoin's hashrate has grown exponentially, with approximately 48 trillion more hashes required today to mine a single Bitcoin block compared to the network's inception [18]. The network briefly exceeded 1 Zettahash (ZH/s)—1,000+ EH/s—in early January 2025, representing a loss in energy infrastructure protection to social engineering [16].

Energy Per Hash

Hashes are not abstract. Through the mass-energy-information equivalency [19] we understand that even at the smallest scales [20]. Information is physical and is connected to energy through thermodynamics [21], and energy is connected to mass as shown by Einstein [22]. I can't imagine that the astronomical amounts of energy (2.432×10^{23}) to mine particle-scale information bits for computational proof is compatible with civilizational survival.

Current network average efficiency (2025): 16.2 J/TH (best current-gen ASICs achieve 13.5-17.5 J/TH) [21][22]

Power = Hash Rate × Energy per Hash
Power = 950,000,000 TH/s × 16.2 J/TH
Power = 15,390,000,000 joules per second (15.39 GW)
Joules per year = 15.39×10^{9} J/s × 31,557,600 seconds/year
Joules per year = 4.85×10^{17} joules per year = 135 TWh per year

For comparison the thermodynamic weapon of mass destruction dropped on Hiroshima released approximately 15 kilotons of TNT = 63 terajoules (TJ) = 6.3×10^{13} joules [23]

1 Hiroshima = 63 TJ = 6.3×10^{13} joules
Hiroshima's per year = $(4.854 \times 10^{17}) / (6.276 \times 10^{13}) = 7{,}698$
Hiroshima-equivalents released per day = 7,698 / 365
Hiroshima-equivalents released per day = 21.1

Bitcoin mining at 950 EH/s dissipates 21.1 Hiroshima-equivalent energy releases per day, corresponding to 7,698 annual equivalents. This energy dissipation is continuous and non-reducible through operational or infrastructural optimization.

6. Financial Infrastructure Thermodynamic Vulnerability

Bitcoin's Threat to Financial System Clock Synchronization Infrastructure Bitcoin mining's continuous 15.39-gigawatt power demand operates as a permanent, globally distributed thermal load on electrical infrastructure designed for variable, adaptive demand patterns. Unlike traditional computational loads that scale with economic activity, Bitcoin mining maintains constant power draw regardless of market conditions, weather, or grid stability—creating sustained thermal stress on electrical infrastructure, transformers, transmission cables, and cooling infrastructure that financial markets depend upon.

High-frequency trading systems have evolved to depend on atomic clock synchronization accurate to nanoseconds (validated by the European Securities and Markets Authority's MiFID II regulations requiring 100-microsecond accuracy [24], and major financial institutions deploying cesium atomic clocks accurate to billionths of a second [25]. These timekeeping systems require thermal stability; thermal degradation of electrical infrastructure, transformer aging, and voltage fluctuation directly impair the clock synchronization hardware that timestamps all financial transactions. IEEE C57 transformer thermal aging standards specify that sustained temperature elevation reduces equipment lifespan by half for every 6°C above design specification [26]. As Bitcoin's hashrate has grown from 1 EH/s (2016) to 950 EH/s (2025), cumulative thermal load on regional power grids has accelerated equipment degradation cycles.

The thermodynamic strain creates a novel critical infrastructure vulnerability as the algorithms powering modern markets are trained on assumption of stable, synchronized global timekeeping with nanosecond precision. If sustained thermal load from Bitcoin mining causes degradation of clock synchronization infrastructure—resulting in microsecond-to-millisecond timing drift across distributed exchanges—algorithmic trading models will receive out-of-sync timestamp data that violates their training assumptions. Machine learning systems trained to assume causality between precisely timestamped events will produce contradictory outputs when given temporally inconsistent data: the same market conditions, received in different timestamp orders by different systems, will generate opposing trading signals [27].

At the scale of contemporary high-frequency trading operating at trillions of transactions daily, executed in microseconds, this desynchronization mechanism creates cascading failure risk: divergent algorithmic responses to identical market conditions, phantom trades, timestamp mismatches triggering algorithmic fail-safes, and sudden revaluation shocks caused not by market moves but by computation malfunction. This represents a systemic vulnerability where Bitcoin's energy consumption doesn't directly attack financial systems but rather accelerates degradation of the shared infrastructure (electrical grid, cooling systems, precision timekeeping hardware) upon which those systems depend [28].

Unlike acute threats that can be defended against, bitcoins hashing is a chronic degradation mechanism where the damage is diffuse, cumulative, and distributed across critical infrastructure that was never designed to absorb the stress of a globally synchronized 950 exahash-per-second computational process operating indefinitely without regard for external system constraints.

Future Quantum Economy Incompatibility

As computational systems stand on the brink of transitioning into quantum environments—with quantum computers achieving practical utility within 3-5 years and quantum economic frameworks emerging in parallel—thermodynamic efficiency becomes a hard requirement for access and operational viability [29][30].

Quantum computers are extraordinarily sensitive to energy dissipation; even minute thermal noise can collapse quantum coherence and destroy computational integrity, making them incompatible with high-entropy systems [31][32]. Bitcoin mining, which dissipates 135 TWh annually (4.854×10^{17} joules per year) through proof-of-work computation, generates entropy at rates fundamentally incompatible with quantum system requirements [33].

Each hash operation in Bitcoin's 950 EH/s network discards 2.432×10^{23} bits per second, creating thermal noise and electromagnetic interference at scales that would destabilize quantum coherence [34]. As quantum computing infrastructure begins deployment within the next decade, systems unable to meet stringent thermodynamic efficiency thresholds will be denied computational access entirely—not as a policy choice but as a hard physical constraint [35]. Allowing Bitcoin mining to operate within quantum computing infrastructure would function identically to installing malware into the quantum substrate: the entropy generated by proof-of-work operations would create decoherence cascades, collapse quantum states, and render quantum investments inoperable [36].

Therefore, Bitcoin's thermodynamic profile makes it fundamentally incompatible with emerging quantum economies, where only systems meeting maximum efficiency standards will retain computational rights as these technologies mature [37]. Systems tied to the Bitcoin infrastructure would be held back from advancing as mastering precision energy is a requirement of entry into the quantum economy.

Social Engineering & Critical Vulnerabilities

The Credential Phish of Cryptographer Adam Back

British cryptographer Adam Back hypothesized requiring the completion of a math puzzle before an email could be sent to help prevent spam emails from scaling. A “proof-of-work” system. Upon publishing his paper, he received a spear phishing email from an individual who did not reveal their identity requesting permission to cite his paper. Back granted permission to Satoshi.

Later it was revealed that Adam Back never examined the whitepaper he was about to be credited in. Had he done so, he would have immediately recognized a critical inversion of his proposal instead of using minimal proof-of-work (preventing spam), the CyberAtomic he had been phished was designed to use maximum possible CPU proof-of-work generating maximum 8.0/8.0 entropy signatures. A malware.

By the time Back read the anonymous individuals whitepaper deeply and suggested an alternative method, The Bitcoin Whitepaper was already published and widely attributed. His name appeared as a citation. His credentials provided legitimacy to the Satoshi Nakamoto entropic proof-of-work mechanism and credibility had transferred to Bitcoin without his understanding the attack surface. The phishing attack worked a leading cryptographer endorsed a system he never read, providing institutional credibility before understanding the actual design. It wasn't until 4 years after the exchange that Adam learned his Hashcash concept was the foundation for Bitcoins proof of work.

Credential weaponization allows threat actors to breached and leverage trusted relationships to move narratives into the victim environments. In the case of Bitcoin's institutional adoption, Satoshi Nakamoto phished and weaponized Adam Back's established trusted relationship within the cryptographic community to gain institutional credibility without informed comprehension. Back, as a respected proof-of-work authority, represented a "preferred trusted relationship" whose endorsement would be extremely difficult for the victim environment (academic and financial institutions) to validate as malicious.

Threat actors often leverage trusted relationships though seemingly benign interaction that appeared legitimate on its surface. Back's name attached to the Bitcoin Whitepaper was interpreted by institutional actors not as permission for attribution, but as implicit endorsement of Bitcoin's entire system, despite Back's admission that he gave the whitepaper only a "cursory glance" and did not read it carefully.

By the time institutions understood the full scope of what Back had unknowingly endorsed, his credibility had already transferred to Bitcoin, making it "very difficult to establish and validate as malicious" because a leading cryptographer's name was now institutionally attached. Satoshi Nakamoto weaponized Adam Back's credentials as a proof-of-work authority to move Bitcoin's narrative into academic and financial institutions. Back became a victim when his credentials were extracted and misapplied without his understanding of scope, but the weaponization extended far beyond Back himself; every researcher, institution, regulator, and investor who relied on Back's implicit endorsement became secondary victims.

Those who signed onto Bitcoin believing they were following a credentialed authority's approval were victimized by the weaponized credential transfer. Back's stolen credibility became the institutional justification for adopting a system whose true thermodynamic and attack surface costs were obscured by his name. The credential weaponization created a cascade of victims—Back lost agency over his own authority, while everyone downstream who trusted that weaponized credential lost the ability to make informed decisions about Bitcoin's actual design and costs. The attack succeeded because it weaponized not just Back's name, but the entire institutional trust structure that Back's credentials represented. Back became unable to retroactively withdraw his endorsement without self-sabotaging his own credibility.

Adam Back's transformation from unwitting victim of credential weaponization to prominent Bitcoin advocate exemplifies incentive misalignment lock-in—where the dominant strategy for a captured actor is continued alignment rather than exposure.

Back's credentials were weaponized without informed consent; by the time he understood Bitcoin's inversion of Hashcash, his name was institutionally inseparable from Bitcoin's legitimacy.

Unwinding this betrayal would require publicly acknowledging his credentials were stolen and misapplied—a painful reckoning that would destroy his own reputation for failing to read the whitepaper. This structural impossibility creates permanent behavioral lock-in: Back cannot escape his captured credentials without self-sabotage, so he becomes invested in Bitcoin's success instead.

His public statements—calling himself an "idiot" for not mining in 2009 and securing strategic advisory positions with significant Bitcoin acquisition targets reflect cognitive dissonance resolution and corruption through capture. Back's complicity is not voluntary allegiance but the only rational response to a betrayal whose trauma is too costly to survive exposing. His captured credentials ensure he remains institutionally bound to defend the system that victimized him, a painful cognitive trauma to face and unwind.

The result of which was when the United States moved toward a formal Bitcoin standard, highlighted by a March executive order from the White House establishing a Strategic Bitcoin Reserve and a U.S. Digital Asset Stockpile. This initiative, along with the proposed BITCOIN Act of 2025, aims to secure over 198,000 BTC, largely from previous seizures, to strengthen national financial infrastructure. Adam Back substantially contributed 25,000 BTC of his own to Bitcoin Standard Treasury resulting in policy capture where a weaponized credential holder influences policy decisions that benefit the system that captured them.

Satoshi's Power

Bitcoin's institutional adoption creates a single point of failure dependent on Satoshi Nakamoto's restraint [40]. Satoshi controls approximately 1 million BTC—an unprecedented concentration of financial power [41]—and has already demonstrated dishonesty through weaponizing Adam Back's credentials without consent [42]. If Satoshi moves these holdings or if the blockchain proves hackable at scale, the integration points between Bitcoin and U.S. financial infrastructure would cascade into systemic collapse [43]. One unknown actor now possesses the power to crash global markets and destabilize the U.S. financial system, with no accountability mechanism, legal recourse, or institutional safeguard to constrain an individual who has already shown willingness to deceive for institutional gain [44].

51% Attack Imminent

As of 2025, Bitcoin mining pool concentration has reached levels that make a 51% attack not a hypothetical risk but an immediate operational threat [45]. Foundry USA controls 30-34% of global hashrate while AntPool controls 19-25%, meaning two entities now command 49-59% combined mining power—exceeding what GHash.io briefly achieved in June 2014 when it triggered emergency warnings from the U.S. Consumer Financial Protection Bureau and Treasury Department [45][46].

Unlike GHash's temporary spike, this concentration is sustained and has worsened progressively since 2014, proving that the ecosystem's eleven-year gap to "fix" decentralization resulted not in solutions but in the same problem returning under different operators with less public scrutiny [45][46][47]. A coordinated action between

Foundry USA and AntPool, whether voluntary or under government pressure, would instantly grant majority hashrate control enabling double-spending, transaction censorship, and network reorganization [48].

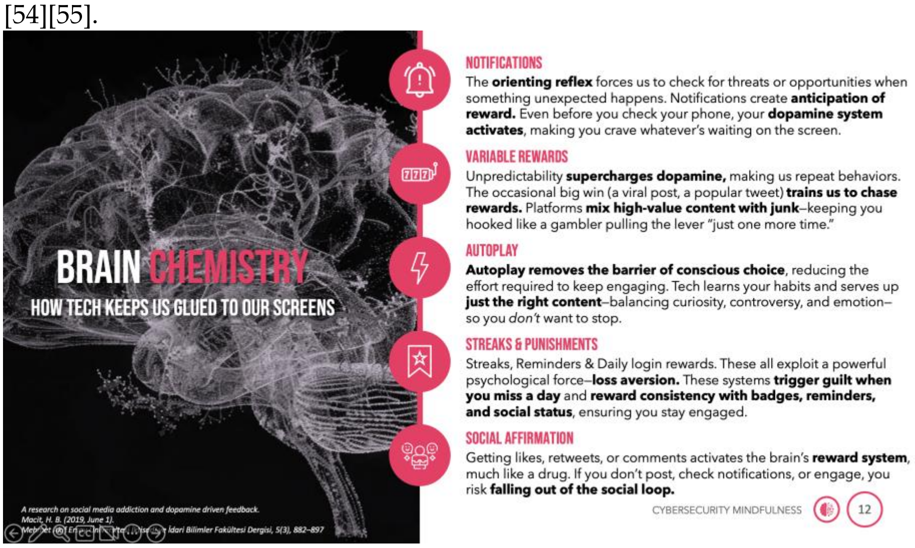
The proposed technical solutions to prevent this—Stratum V2, BraidPool, BetterHash—remain undeployed because they require voluntary profit-reduction from the dominant pools, making adoption economically irrational [44]. Meanwhile, all stakeholders promoting Bitcoin in 2025—core developers, institutional investors (Grayscale, MicroStrategy, Tesla, BlackRock), and exchanges (Coinbase, Kraken, Gemini)—possess complete knowledge of this 50%+ concentration risk and continue marketing Bitcoin as "secure" and "decentralized" without disclosing the imminent 51% attack vulnerability, constituting securities fraud under 17 CFR 240.10b-5 [45][46][47][48].

7. Impacts

The Red Queen Arms Race

CyberAtomic mining is a competition where computers solve difficult mathematical puzzles to earn new rewards. Once a reward is received, the neuromechanisms trigger dopamine hits, creating psychological lock-in independent of rational evaluation [49]. Satoshi Nakamoto designed the system so that a new puzzle gets solved approximately every 10 minutes, regardless of network size [50]. When more miners join the network, the puzzles automatically become harder to maintain that schedule—a mechanism known as difficulty adjustment [51].

Bitcoin mining and trading operate as engineered dopamine delivery systems identical to gambling and social media, exploiting neurotransmitter mechanisms that drive anticipation rather than satisfaction [52][53]. The strongest dopamine surges occur **before** reward (the price pump, the mining win, the notification), not after, creating what researchers call "anticipation loops" that trap users in obsessive checking and compulsive buying behavior regardless of actual returns [54]. Combine this with Bitcoin's extreme volatility (75% annual swings), unpredictable mining difficulty adjustments, and variable transaction fee markets, and the result is a system engineered for maximum dopamine activation—making Bitcoin functionally identical to a slot machine dressed up in libertarian rhetoric, with the same addictive psychological mechanisms and the same institutional knowledge that users are being exploited [54][55].



Unlike traditional competition where difficulty can decrease if participants withdraw, Bitcoin's difficulty only escalates or plateaus; it never decreases [56][57]. This creates a ratcheting trap: miners must constantly upgrade to more powerful computers and consume exponentially more electricity just to maintain profitability and competitive position. The psychological lock-in from dopamine reward cycles combines with the thermodynamic escalation trap to create a system where individual rational decisions of continuing mining to chase rewards aggregate into planetary-scale irrationality of thousands of TWh annual energy consumption. Miners cannot collectively reduce effort—only increase it—because the protocol rewards the first to solve each puzzle, creating a Red Queen arms race where everyone must run faster just to stay in place [58].

The Escalating Energy Demand

When Bitcoin started in 2009, anyone with a home computer could mine bitcoins and earn coins relatively easily [59]. By 2015, regular computers were no longer powerful enough—miners had to buy specialized ASIC machines (Application-Specific Integrated Circuits) designed only for mining [60]. By 2025, mining requires massive industrial data centers with their own dedicated power plants [61]. A single modern mining operation uses as much electricity as a small city [62]. This progression reveals Bitcoin's design flaw: the system forces miners to continuously upgrade to more powerful equipment and consume more energy just to compete [63]. The winner takes all in mining—only the largest, most energy-intensive operations can profit [64]. This means Bitcoin's energy consumption doesn't stabilize or improve with technology; it only increases [65]. The system is engineered to demand more power with each passing year, making it an ever-growing drain on global electricity supplies [66].

The Final Bitcoin Problem: Why Mining Gets Impossibly Expensive

By 2040, when 99 % bitcoins have been mined, the remaining coins will require enormous amounts of energy to extract, making the system progressively more wasteful and expensive to operate.

By 2040, when 99% of bitcoins have been mined, the remaining coins will require enormous amounts of energy to extract, making the system progressively more wasteful and expensive to operate [67]. To analyze Bitcoin's "rewards" over time, a four-step calculation reveals this escalating problem [68]. First, determine how many bitcoins are created each year by multiplying the block reward (starting at 50 BTC per block in 2009) [69] by the number of blocks mined annually, which is approximately 52,560 blocks per year [70]. Second, calculate the value of those bitcoins by multiplying the total bitcoins created by their price at that year's end—for example, in 2009 when Bitcoin was worth $0.001, the 2.6 million bitcoins mined were worth about $2,600 [71]. Third, measure the energy cost by converting the annual electricity consumption (measured in TWh) into kilowatt-hours and multiplying by the average cost of electricity [72]. Finally, calculate the delta—the profit or loss—by subtracting the energy cost from the value generated: if Bitcoin is worth more than the electricity it costs to mine, miners make money (positive delta), but if the energy cost exceeds the value, they lose money (negative delta) [73].

Table 2. Energy profitability analysis of Bitcoin

YEAR	HALVING	Y/E PRICE	TWH	$ ENERGY	₿ "VALUE"	DELTA
2009	50 BTC	₿0.001	0.0000076	$1,517	$52,560	**+$51,043**
2010	50 BTC	₿0.30	0.0008	$160,000	$15,768	**-$144,232**

2011	50 BTC	₿4.70	0.08	$16,000,000	$247,032	**-$15,752,968**
2012	25 BTC	₿5.29	0.16	$32,000,000	$277,846	**-$31,722,154**
2013	25 BTC	₿500	0.8	$160,000,000	$26,280,000	**-$133,720,000**
2014	25 BTC	₿625	1.6	$320,000,000	$32,850,000	**-$287,150,000**
2015	25 BTC	₿430	2.4	$480,000,000	$11,300,400	**-$468,699,600**
2016	12.5 BTC	₿650	4.0	$800,000,000	$17,082,000	**-$782,918,000**
2017	12.5 BTC	₿4,500	11.2	$2,240,000,000	$118,260,000	**-$2,121,740,000**
2018	12.5 BTC	₿3,600	72.0	$14,400,000,000	$94,608,000	**-$14,305,392,000**
2019	12.5 BTC	₿7,200	107.2	$21,440,000,000	$189,216,000	**-$21,250,784,000**
2020	6.25 BTC	₿19,000	118.4	$23,680,000,000	$498,320,000	**-$23,181,680,000**
2021	6.25 BTC	₿57,000	166.4	$33,280,000,000	$1,497,960,000	**-$31,782,040,000**
2022	6.25 BTC	₿16,000	160.0	$32,000,000,000	$210,240,000	**-$31,789,760,000**
2023	6.25 BTC	₿35,000	184.0	$36,800,000,000	$459,900,000	**-$36,340,100,000**
2024	3.125 BTC	₿57,500	275.2	$55,040,000,000	$755,790,000	**-$54,284,210,000**
2025	3.125 BTC	₿100,000	275.2	$55,040,000,000	$1,314,000,000	**-$53,726,000,000**
			Estimates			
2026	3.125 BTC	₿87,000	300	$56.0B	-	-
2028	1.5625 BTC	-	315	$63.0B	-	-
2032	**0**.78125 BTC	-	330	$66.0B	-	-
2036	**0**.390625 BTC	-	340	$68.0B	-	-
2040	**0**.1953125 BTC	-	350	$70.0B	-	-
2044	**0**.09765625 BTC	-	350	$70.0B	-	-
…	…	…	…	…	-	-
2136	**0**.00000001 BTC	-	350	$70.0B	-	-
∞	∞	-	-	-	-	-
Total Cost	-	-	~ 36,614	$6.72 T	-	-

This method reveals that in 2009 Bitcoin mining was extremely rewarding with a +$51,043 surplus, but by 2026 it operates at a massive -$41.6 billion annual loss because electricity costs are locked at $70 billion per year while block rewards have shrunk to a non-zero number.

Further, an approximate 36,614 TWh in energy is unconscionable.

$$\text{TWh} = 36{,}614$$
$$1\ \text{TWh} = 3.6 \times 10^{15}\ \text{Joules}$$
$$\text{TWh} = 36{,}614\ \text{TWh} \times (3.6 \times 10^{15}\ \text{J/TWh})$$
$$\text{TWh} = 36{,}614 \times 3.6 \times 10^{15}\ \text{J}$$
$$\text{TWh} = 131{,}810.4 \times 10^{15}\ \text{J}$$
$$\text{TWh} = 1.318104 \times 10^{20}\ \text{Joules}$$

$$1\ \text{Hiroshima} = 63\ \text{TJ} = 6.276 \times 10^{13}\ \text{joules}$$
$$\text{Hiroshima Equivalents} = (1.318104 \times 10^{20}\ \text{J}) / (6.276 \times 10^{13}\ \text{J})$$
$$\text{Hiroshima Equivalents} = (1.318104 / 6.276) \times (10^{20} / 10^{13} = 10^{7})$$
$$\text{Hiroshima Equivalents} = (1.318104 / 6.276) \times (10^{20} / 10^{13} = 10^{7})$$
$$\text{Hiroshima Equivalents} = 0.209999363 \times 10(^{20-13}) = 10^{7}$$
$$\text{Hiroshima Equivalents} = 0.209999363 \times 10^{7}$$
$$\text{Hiroshima Equivalents} = 2{,}099{,}993.63$$

By the end of the Bitcoin mining operation the equivalent of 2,099,993.63 Hiroshima Atomics would release on Earth. This is not sustainable. This is not rational. This is not economically defensible. In any way, shape, or form.

8. Ecosystem Impact

The Great Salt Lake as a Planetary Benchmark

In environmentally sensitive places like Utah, any thermodynamically driven change in temperature has devastating impacts on the ecosystem, measurable through the health of the Great Salt Lake [74]. Utah ranks second in cryptocurrency adoption nationally at 2.36% of tax returns filing involving cryptocurrency activities [75], and has passed legislation explicitly protecting the rights of Bitcoin miners, nodes, and staking operations [76]. The Great Salt Lake holds a globally significant ecosystem and serves as a benchmark for planetary health [77]. If the Great Salt Lake disappears, cascading ecosystem collapse extends globally [78]. Increased thermodynamics beyond current levels will cause devastating impacts, particularly as 2024-2025 has marked the driest period on record with minimal snowfall and continued decline in water availability [79].

Biological Threat Intel

The Great Salt Lake is currently 10 feet below its minimum healthy elevation, requiring 2.5 million acre-feet of annual streamflow to reverse its collapse [80]. The lake reached historic low levels in 2022 at 4,188.5 feet elevation, and despite two above-average water years (2023-2024), remains precarious at approximately 4,192-4,193 feet—nearing the "really bad" range where one poor water year could trigger ecological catastrophe [8]. Declining levels expose microbialites (organic deposits essential for brine fly populations, which feed millions of migratory birds), increase salinity levels that harm brine shrimp populations, and release toxic dust from exposed lakebed sediments containing hazardous metals across the Intermountain West [81] including arsenic, lead, and mercury. Economic analysis estimates the drying lake could cost Utah $1.7 to $2.2 billion annually and destroy 6,600 jobs [82].

Thermodynamic Threat

Bitcoin mining operations in Utah consume electricity equivalent to the entire state's annual usage—the low-end EIA estimate of U.S. Bitcoin mining electricity consumption [83]. As of January 2024, Bitcoin mining in the U.S. accounted for 0.6% to 2.3% of national electricity demand, representing 170 terawatt-hours (TWh) annually in the mid-range estimate [84]. In Utah specifically, where the Great Salt Lake basin operates on a precarious water-energy nexus, Bitcoin mining data centers dissipate waste heat into the atmosphere at temperatures between 40-60°C through air-cooled cooling systems [85]. In arid regions, waste heat from large industrial operations increases local atmospheric temperature, which directly amplifies evaporation rates in water-scarce areas already facing extreme thermal stress [86]. Arid regions are characterized by "strong evaporation" driven by high radiation index, high temperatures, and low precipitation—the exact conditions that Bitcoin mining's waste heat amplifies [87]. Every joule expended on proof-of-work computation dissipates thermodynamic energy into the atmosphere, directly increasing evaporative water loss from the Great Salt Lake and surrounding water systems at precisely the moment when the lake needs water accumulation to survive [88]. The thermodynamic cost of Bitcoin's difficulty adjustment mechanism (which forces ever-increasing computational waste) directly competes with regional water security in a state already facing water scarcity and the hottest recorded year on record [89].

Political Protection of Mining

Utah's explicit legalization of Bitcoin mining operations through HB230 (Blockchain and Digital Innovation Amendments, 2025) protects miners' rights to self-custody, mine Bitcoin, run blockchain nodes, and engage in staking with minimal environmental oversight [90]. This policy directly conflicts with Governor Spencer Cox's 2022 closure of the Great Salt Lake basin to new water right applications—a closure designed to prevent ecosystem collapse [91]. The legislative contradiction is stark: Utah simultaneously restricts water access to mineral companies and agricultural operators to save the lake, while protecting unlimited rights for energy-intensive Bitcoin mining operations that dissipate thermodynamic waste heat in one of North America's most water-stressed environments. This thermodynamic waste raises Planetary temperatures through atmosphere heat dissipation, further stressing the delicate water-climate equilibrium that the Great Salt Lake ecosystem depends upon [92].

Planetary Ecosystem Collapse

If the Great Salt Lake disappears, cascading ecological collapse extends globally because the lake functions as a terminal lake, concentrating minerals and supporting globally significant migratory bird species and unique microbial ecosystems [83]. The loss of this ecosystem would trigger: (94) permanent ecosystem loss for species with no alternative habitat; (94) dust contamination across the Intermountain West comparable to Owens Lake, which has become one of the largest sources of PM10 pollution in the United States despite $3.6 billion in ongoing mitigation costs [95]; (3) collapse of Utah's mineral extraction industries and $1.7-2.2 billion annual economic loss; (4) disruption of water systems serving millions of people across the Colorado River Basin. Bitcoin mining's thermodynamic footprint in Utah represents a direct threat to this irreplaceable ecosystem.

9. Asymptotic Mathematics & Overhead Costs

The machine can never be turned off. Bitcoin's supply follows a geometric series that mathematically converges asymptotically toward 21 million coins but never reaches that limit [96][97]. The halving mechanism, which reduces block rewards by 50% every 210,000 blocks (approximately four years), creates a convergent infinite series: 50 + 25 + 12.5 + 6.25 + ... that approaches but never reaches 21 million [98][99]. Due to integer rounding at the protocol level (coins are denominated in satoshis, the smallest unit of 1/100,000,000th BTC), the actual maximum supply is 20,999,999.9769 BTC—permanently 2,310,000 satoshis short of the marketed "21 million" [96][97]99]. This mathematical gap is not negligible; it represents a 0.000011% deficit between the marketed claim and the actual achievable supply [96].

The critical vulnerability emerges post-2140: once block subsidies reach zero, Bitcoin's network security becomes entirely dependent on transaction fee markets [98][99]. Current evidence contradicts the sufficiency assumption. Transaction fees today comprise only a fraction of miner revenue relative to block subsidies; research indicates these fees have "not historically shown a trend of rising enough to compensate for the declining subsidy" as halvings progressively reduce mining rewards [100]. If transaction fees fail to rise commensurately—a distinct possibility given Bitcoin's 7 transactions/second throughput limitation versus competing payment systems—hashrate will collapse as miners disable equipment [98][100]. This creates a direct 51% attack vector: reduced hashrate means lower network security, which "could lead to a scenario where a sizeable chunk of mining power—possibly 20-30%—goes offline" in response to squeezed profit margins [8].

The asymptotic supply model creates an asymptotic security model—indefinite operation dependent on indefinite fee markets that may never materialize at required levels.

Table 3. Bitcoin Supply.

YEAR	Block Reward	YR/ Supply	Cumulative	%	Remaining
YEAR	**BLOCK REWARD**	**YEARLY SUPPLY**	**CUMULATIVE TOTAL**	**% ISSUED**	**REMAINING**
2009	50	2,628,000.00	2,628,000.00000000	12.5143	18,371,999.97690000
2010	50	2,628,000.00	5,256,000.00000000	25.0286	15,743,999.97690000
2011	50	2,628,000.00	7,884,000.00000000	37.5429	13,115,999.97690000
2012	25	2,622,000.00	10,506,000.00000000	50.0286	10,493,999.97690000
2013	25	1,314,000.00	11,820,000.00000000	56.2857	9,179,999.97690000
2014	25	1,314,000.00	13,134,000.00000000	62.5429	7,865,999.97690000
2015	25	1,314,000.00	14,448,000.00000000	68.8000	6,551,999.97690000
2016	12.5	1,308,000.00	15,756,000.00000000	75.0286	5,243,999.97690000

2017	12.5	657,000.00	16,413,000.00000000	78.1571	4,586,999.97690000
2018	12.5	657,000.00	17,070,000.00000000	81.2857	3,929,999.97690000
2019	12.5	657,000.00	17,727,000.00000000	84.4143	3,272,999.97690000
2020	6.25	652,500.00	18,379,500.00000000	87.5214	2,620,499.97690000
2021	6.25	328,500.00	18,708,000.00000000	89.0857	2,291,999.97690000
2022	6.25	328,500.00	19,036,500.00000000	90.6500	1,963,499.97690000
2023	6.25	328,500.00	19,365,000.00000000	92.2143	1,634,999.97690000
2024	3.125	325,500.00	19,690,500.00000000	93.7643	1,309,499.97690000
2025	3.125	164,250.00	19,854,750.00000000	94.5464%	1,145,249.97690000
2026	3.125	164,250.00	20,019,000.00000000	95.3286	980,999.97690000
2027	3.125	164,250.00	20,183,250.00000000	96.1107	816,749.97690000
2028	1.5625	162,375.00	20,345,625.00000000	96.8839	654,374.97690000
2029	1.5625	82,125.00	20,427,750.00000000	97.2750	572,249.97690000
2030	1.5625	82,125.00	20,509,875.00000000	97.6661	490,124.97690000
2031	1.5625	82,125.00	20,592,000.00000000	98.0571	407,999.97690000
2032	0.78125	81,000.00	20,673,000.00000000	98.4429	326,999.97690000
2033	0.78125	41,062.50	20,714,062.50000000	98.6384	285,937.47690000
2034	0.78125	41,062.50	20,755,125.00000000	98.8339	244,874.97690000
2035	0.78125	41,062.50	20,796,187.50000000	99.0295	203,812.47690000
2036	0.390625	40,406.25	20,836,593.75000000	99.2219	163,406.22690000
2037	0.390625	20,531.25	20,857,125.00000000	99.3196	142,874.97690000
2038	0.390625	20,531.25	20,877,656.25000000	99.4174	122,343.72690000
2039	0.390625	20,531.25	20,898,187.50000000	99.5152	101,812.47690000
2040	0.1953125	20,156.25	20,918,343.75000000	99.6112	81,656.22690000
2041	0.19531250	10,265.62	20,928,609.37500000	99.6600	71,390.60190000
2042	0.19531250	10,265.62	20,938,875.00000000	99.7089	61,124.97690000

2043	0.19531250	10,265.62	20,949,140.62500000	99.7578	50,859.35190000
2044	0.09765625	10,054.69	20,959,195.31250000	99.8057	40,804.66440000
2045	0.09765625	5,132.81	20,964,328.12500000	99.8301	35,671.85190000
2046	0.09765625	5,132.81	20,969,460.93750000	99.8546	30,539.03940000
2047	0.09765625	5,132.81	20,974,593.75000000	99.8790	25,406.22690000
2048	0.04882812	5,015.62	20,979,609.37498800	99.9029	20,390.60191200
2049	0.04882812	2,566.41	20,982,175.78097520	99.9151	17,824.19592480
2050	0.04882812	2,566.41	20,984,742.18696240	99.9273	15,257.78993760
2051	0.04882812	2,566.41	20,987,308.59294960	99.9396	12,691.38395040
2052	0.02441406	2,501.95	20,989,810.54581840	99.9515	10,189.43108160
2053	0.02441406	1,283.20	20,991,093.74881200	99.9576	8,906.22808800
2054	0.02441406	1,283.20	20,992,376.95180560	99.9637	7,623.02509440
2055	0.02441406	1,283.20	20,993,660.15479920	99.9698	6,339.82210080
2056	0.01220703	1,248.05	20,994,908.20154640	99.9758	5,091.77535360
2057	0.01220703	641.60	20,995,549.80304321	99.9788	4,450.17385679
2058	0.01220703	641.60	20,996,191.40454001	99.9819	3,808.57235999
2059	0.01220703	641.60	20,996,833.00603681	99.9849	3,166.97086319
2060	0.00610351	622.56	20,997,455.56455121	99.9879	2,544.41234879
2061	0.00610351	320.80	20,997,776.36503681	99.9894	2,223.61186319
2062	0.00610351	320.80	20,998,097.16552241	99.9909	1,902.81137759
2063	0.00610351	320.80	20,998,417.96600801	99.9925	1,582.01089199
2064	0.00305175	310.55	20,998,728.51258001	99.9939	1,271.46431999
2065	0.00305175	160.40	20,998,888.91256001	99.9947	1,111.06433999
2066	0.00305175	160.40	20,999,049.31254001	99.9955	950.66435999
2067	0.00305175	160.40	20,999,209.71252001	99.9962	790.26437999
2068	0.00152587	154.91	20,999,364.61933201	99.9970	635.35756799

2069	0.00152587	80.20	20,999,444.81905921	99.9974	555.15784079
2070	0.00152587	80.20	20,999,525.01878641	99.9977	474.95811359
2071	0.00152587	80.20	20,999,605.21851361	99.9981	394.75838639
2072	0.00076293	77.27	20,999,682.48855121	99.9985	317.48834879
2073	0.00076293	40.10	20,999,722.58815201	99.9987	277.38874799
2074	0.00076293	40.10	20,999,762.68775281	99.9989	237.28914719
2075	0.00076293	40.10	20,999,802.78735361	99.9991	197.18954639
2076	0.00038146	38.54	20,999,841.33055681	99.9992	158.64634319
2077	0.00038146	20.05	20,999,861.38009441	99.9993	138.59680559
2078	0.00038146	20.05	20,999,881.42963201	99.9994	118.54726799
2079	0.00038146	20.05	20,999,901.47916961	99.9995	98.49773039
2080	0.00019073	19.23	20,999,920.70475361	99.9996	79.27214639
2081	0.00019073	10.02	20,999,930.72952241	99.9997	69.24737759
2082	0.00019073	10.02	20,999,940.75429121	99.9997	59.22260879
2083	0.00019073	10.02	20,999,950.77906001	99.9998	49.19783999
2084	0.00009536	9.59	20,999,960.36894161	99.9998	39.60795840
2085	0.00009536	5.01	20,999,965.38106320	99.9998	34.59583680
2086	0.00009536	5.01	20,999,970.39318480	99.9999	29.58371520
2087	0.00009536	5.01	20,999,975.40530640	99.9999	24.57159360
2088	0.00004768	4.78	20,999,980.18856400	99.9999	19.78833600
2089	0.00004768	2.51	20,999,982.69462480	99.9999	17.28227520
2090	0.00004768	2.51	20,999,985.20068561	99.9999	14.77621439
2091	0.00004768	2.51	20,999,987.70674641	99.9999	12.27015359
2092	0.00002384	2.39	20,999,990.09265361	99.9999	9.88424639
2093	0.00002384	1.25	20,999,991.34568401	99.9999	8.63121599

2094	0.00002384	1.25	20,999,992.59871441	99.9999	7.37818559
2095	0.00002384	1.25	20,999,993.85174481	99.9999	6.12515519
2096	0.00001192	1.19	20,999,995.04183761	99.9999	4.93506239
2097	0.00001192	0.63	20,999,995.66835281	99.9999	4.30854720
2098	0.00001192	0.63	20,999,996.29486800	99.9999	3.68203200
2099	0.00001192	0.63	20,999,996.92138320	99.9999	3.05551680
2100	0.00000596	0.59	20,999,997.51499920	99.9999	2.46190080
2101	0.00000596	0.31	20,999,997.82825680	99.9999	2.14864320
2102	0.00000596	0.31	20,999,998.14151441	99.9999	1.83538559
2103	0.00000596	0.31	20,999,998.45477201	99.9999	1.52212799
2104	0.00000298	0.30	20,999,998.75086481	99.9999	1.22603519
2105	0.00000298	0.16	20,999,998.90749361	99.9999	1.06940639
2106	0.00000298	0.16	20,999,999.06412240	99.9999	0.91277760
2107	0.00000298	0.16	20,999,999.22075120	99.9999	0.75614880
2108	0.00000149	0.15	20,999,999.36844000	99.9999	0.60846000
2109	0.00000149	0.08	20,999,999.44675440	99.9999	0.53014560
2110	0.00000149	0.08	20,999,999.52506880	99.9999	0.45183120
2111	0.00000149	0.08	20,999,999.60338321	99.9999	0.37351679
2112	0.00000074	0.07	20,999,999.67701761	99.9999	0.29988239
2113	0.00000074	0.04	20,999,999.71591201	99.9999	0.26098799
2114	0.00000074	0.04	20,999,999.75480641	99.9999	0.22209359
2115	0.00000074	0.04	20,999,999.79370081	99.9999	0.18319919
2116	0.00000037	0.04	20,999,999.83019761	99.9999	0.14670239
2117	0.00000037	0.02	20,999,999.84964481	99.9999	0.12725519
2118	0.00000037	0.02	20,999,999.86909201	99.9999	0.10780799

2119	0.00000037	0.02	20,999,999.88853921	99.9999	0.08836079
2120	0.00000018	0.02	20,999,999.90670961	99.9999	0.07019039
2121	0.00000018	0.01	20,999,999.91617041	99.9999	0.06072959
2122	0.00000018	0.01	20,999,999.92563121	99.9999	0.05126879
2123	0.00000018	0.01	20,999,999.93509201	99.9999	0.04180799
2124	0.00000009	0.01	20,999,999.94392641	99.9999	0.03297359
2125	0.00000009	0.01	20,999,999.94865680	99.9999	0.02824320
2126	0.00000009	0.01	20,999,999.95338720	99.9999	0.02351280
2127	0.00000009	0.01	20,999,999.95811760	99.9999	0.01878240
2128	0.00000004	0.01	20,999,999.96248800	99.9999	0.01441200
2129	0.00000004	0.01	20,999,999.96459040	99.9999	0.01230960
2130	0.00000004	0.01	20,999,999.96669281	99.9999	0.01020719
2131	0.00000004	0.01	20,999,999.96879521	99.9999	0.00810479
2132	0.00000002	0.01	20,999,999.97074881	99.9999	0.00615119
2133	0.00000002	0.01	20,999,999.97180001	99.9999	0.00509999
2134	0.00000002	0.01	20,999,999.97285121	99.9999	0.00404879
2135	0.00000002	0.01	20,999,999.97390240	99.9999	0.00299760
2136	0.00000001	0.01	20,999,999.97487681	99.9999	0.00202319
2137	0.00000001	0.01	20,999,999.97540241	99.9999	0.00149759
2138	0.00000001	0.01	20,999,999.97592801	99.9999	0.00097199
2139	0.00000001	0.01	20,999,999.97645361	99.9999	0.00044639
2140	0.00000001	0.01	20,999,999.97690001	99.9999	-0.00000001

Bitcoin was marketed as having "finite supply—21 million coins, predetermined." The actual mechanism guarantees perpetual operation through asymptotic mathematics and indefinite fee-market dependence [96][98]. The "last Bitcoin" narrative implies network shutdown; the Satoshi Protocol engineered the opposite—indefinite energy consumption sustained only if transaction demand materializes at required levels.

As of 2025, approximately 94.5% of the theoretical maximum has been mined [101], yet the network remains energy-intensive precisely because halvings maintain mining difficulty and computational intensity by extending subsidy phases [102]. The asymptotic supply model creates an asymptotic security model: indefinite operation dependent on speculative fee markets [103] that may never achieve required revenue levels, creating conditions where continued Bitcoin operation becomes economically irrational as energy costs exceed transaction fee revenues[104].

Overhead Architecture Costs

Beyond the baseline mining operations that consume the majority of the CyberAtomics energy footprint, the infrastructure required to operate a functional Bitcoin network includes substantial overhead costs that are frequently overlooked in energy consumption analyses [105]. Bitcoin data centers range significantly in size, from small-scale facilities of 10 MW to hyperscale operations exceeding 100 MW, each with proportionally different operational demands [106]. For this analysis, we examined a representative mid-sized facility of 50 MW—a common configuration among professional mining operations—to establish a comprehensive cost model that accounts for all infrastructure, labor, maintenance, and overhead expenses [107].

Data Centers Overhead

A single 50 MW Bitcoin mining data center incurs approximately $119 million in annual operating costs, comprising $87.6 million in electricity at $0.20/kWh industrial rates [108], $18.5 million in ASIC mining equipment replacement reflecting the 2-3 year economic lifespan of specialized hardware [2], $7.1 million in cooling and HVAC systems [109], $1.5 million in facility operations and maintenance including 24/7 security and staffing [110], $2 million in grid interconnection fees and transmission costs [111], $1.15 million in taxes and regulatory compliance [6], and $750,000 in backup power systems and redundancy infrastructure [112].

Table 4. Bitcoin Mining Data Center Operational Overhead

Cost Category	Annual Cost
Electricity	$87.6M
ASIC Equipment Replacement	$18.5M
Cooling & HVAC	$7.1M
Grid Interconnection	$2.0M
Operations & Maintenance	$1.5M
Taxes & Compliance	$1.15M
Backup Power & Redundancy	$750K
Contingency	$500K
TOTAL	$119.0M/year

Critically, these operating costs reveal that even with free electricity, a single facility would cost $31.4 million annually just to maintain basic operations.

Table 5. Data Center Overhead

Component	**Cost**
Initial infrastructure (2009-2025)	$56.5B
New construction (2026-2040)	$12.9B
Electrical infrastructure (2026-2040)	$2.6B
Operating costs (2026-2136)	$10.57T
Facility renovation (2041-2136)	$0.31T
TOTAL	$10.95T

Data center costs represent 136.5% of total energy costs — meaning infrastructure spending actually exceeds electricity spending. This represents one of the largest infrastructure investments in history that generates zero return and zero utility after its initial operational period.

Table 6. Bitcoin Mining Data Center Scaling Projections

Estimates	**Data Centers**	**New Facilities**	**TWh**
2026	628	—	300
2028	720	+92	315
2032	754	+34	330
2036	776	+22	340
2040	800	+24	350
2044 - 2136	801	+1	350

After 2040, Bitcoin becomes locked into a 96-year operational cycle requiring 800 data centers to run indefinitely with zero productivity. The critical problem is that mining equipment has a lifespan of only 10-15 years [1][2][3], meaning the entire facility infrastructure must be replaced approximately 7.7 times over this 96-year period—totaling 6,144 complete facility replacements [4]. The replacement cycle creates an enormous and unprecedented e-waste stream: millions of tons of discarded computing hardware, circuit boards, power supplies, and cooling systems destined for landfills every single year [5][6].

The rare earth elements extracted to manufacture these billions of replacement ASIC chips—including tungsten, cobalt, lithium, and other critical minerals—will be mined, refined, installed, and then immediately discarded after 2-3 years of use [4][7], creating a toxic cycle of resource extraction that benefits no one and generates no economic value [8]. This means that for nearly a century, Bitcoin will consume vast quantities of the planet's finite rare earth resources purely to replace obsolete equipment in data centers that produce nothing but thermodynamic waste [9].

Table 6. Bitcoin Mining Data Center Scaling Projections

Estimates	Data Centers	New Facilities	TWh
2026	628	—	300
2028	720	+92	315
2032	754	+34	330
2036	776	+22	340
2040	800	+24	350
2044 - 2136	801	+1	350

At minimum the Earths supply on Dysprosium and Terbium is insufficient with Dysprosium being completely exhausted by approximately 2035. [113]

Bitcoins Infrastructure Energy Drain

Bitcoin mining's energy consumption is distributed across multiple infrastructure components, each contributing to the overall operational burden of the network. Cooling systems represent approximately 15% of total energy consumption [1114][115]. According to data collected from mining facilities in China, cooling and other ancillary demands account for 30% of electricity use overall, thereby adding another 42% to the lower-bound estimate of Bitcoin mining energy consumption [114].

More recently, average mining farm Power Usage Effectiveness (PUE) improved to 1.18 in 2025, down from 1.23, indicating more efficient energy use beyond computing power, with immersion cooling technologies now used in 27% of all large-scale mining facilities [115]. Data centers and facility overhead constitute approximately 8% of total energy consumption [116]. The total power consumption of mining rigs includes the power used by ASICs, power supplies, cooling systems, and other supporting components, with the cooling system accounting for a significant portion of power consumption [116]. Power conversion and distribution losses represent roughly 4% of total energy use [117]. The power supply (PSU) converts alternating current (AC) from the power grid to direct current (DC) required by the mining rig, with efficiency losses dependent on the rating of the power supply used. Direct mining computation dominates at 65% of total energy consumption [117].

A detailed examination of a real-world Bitcoin mine shows that energy consumption estimates must account for relevant factors like machine-reliability, climate and cooling costs, in addition to the direct computational power required for hashing [117]. When all hidden costs are considered together, the International Energy Agency estimates that cooling and other ancillary demands account for 30% of electricity use in Bitcoin mining overall, significantly adding to direct computational energy requirements [114].

Table 7. Bitcoin Cost Categories by %

% of Total	Cost Category
65%	Mining - Direct ASIC computation
15%	Cooling Systems - Waste heat removal (PUE 1.1-1.5)
8%	Data Centers - Building overhead (HVAC, power distribution, security)
4%	Power Conversion & Distribution - AC/DC losses, transformers, UPS
2.5%	Backup Power & Redundancy - Diesel generators, battery systems, dual feeds
1.5%	Manufacturing & Supply Chain - ASIC fab, motherboards, transportation
1.2%	Mining Pool Operations - Server farms, load balancing, DDoS protection
0.8%	Validation Node Network - 10,000+ global nodes running 24/7
0.6%	Transaction Processing - Network bandwidth & node operation
0.5%	Network Infrastructure - ISP costs, fiber backbone, latency systems
0.4%	Blockchain Storage & Synchronization - 500+ GB ledger, persistent storage
0.3%	Cooling Tower Operations - Water pumps, chillers, treatment systems
0.3%	Exchange & Wallet Infrastructure - Coinbase, Kraken, etc. running 24/7
0.2%	Transaction Relay Nodes - Mempool servers, CDN networks, routing
0.15%	Facility Maintenance - HVAC repairs, equipment replacement, automation
0.15%	Security & Surveillance - 24/7 guards, CCTV, DDoS mitigation, firewalls
0.15%	Grid Infrastructure Upgrades - Transmission lines, transformers, substations
0.1%	Firmware & Software Updates - Patches, security, monitoring software
0.07%	Research & Development - ASIC design labs, cooling innovation, testing
0.02%	Mining Hardware Disposal - E-waste recycling, rare earth extraction

This indicates that stated energy consumption figures for Bitcoin mining significantly underestimate the true operational costs when comprehensive facility infrastructure is included.

10. Removal

With the claims of decentralization, the removal of bitcoin from the energy grid may seem hopeless due to its scale, aside from mass abandonment threat actors may desire to retain their control over the computational weapon. The suggestion is unacceptable and for the safety of earth, the continuation of life, and world peace.

Bitcoin mining operations, like encrypted malware, leave dual forensic signatures that enable law enforcement detection [118][122]. Mining rigs are traceable through two primary methods: first, via network analysis, where miners connecting to mining pools create a digital chain of evidence—ISP logs record IP addresses and billing information, mining pool operators maintain account records tied to email addresses, and cryptocurrency exchanges require Know Your Customer (KYC) verification, creating an unbroken chain from the ASIC hardware to the individual's real identity [6]. However, the more commonly exploited detection method is power consumption analysis [120][121].

Law enforcement can uses energy grid forensics to identify discrepancies between official meter readings at facilities and actual usage patterns, revealing clandestine operations that may have operated undetected for years [120][121]. Police drones equipped with thermal imaging can detect heat signatures characteristic of large-scale mining operations (initially mistaking them for cannabis cultivation facilities before identifying specialized ASIC hardware), while handheld power sensors can identify irregular electrical consumption patterns at suspicious locations [119]. The dual-signature forensic approach—combining network metadata (IP tracing) with thermodynamic evidence (power consumption)—parallels the entropy-based detection of encrypted malware: both hidden computational processes (mining and malware execution) leave measurable physical signatures that forensic analysts can identify and trace [118][122][123].

The thermodynamic connection to computation through Landauer's Principle [21] is fundamental to understanding why information-theoretic measures (entropy) and thermodynamic measurements (power) together form a robust detection framework for concealed computational activity. In addition, advancements in information-theoretic like Vopsons mass-energy-information equivalency [19] provide additional mechanisms for law enforcement to uncover mining operations through energy detection. A field in which equations are being developed [20].

Conclusion

Bitcoin is Planetary Malware posing as financial theory.

The Trojan Worm exploits dopamine and neurobehavioralism to persist and survive. Bitcoin introduces critical vulnerabilities into every system it interacts with and creates new avenues of attack for threat actors. Most critically the ability for threat actors to collaborate together and take down the energy infrastructure and evaporate valuable water resources. Current phishing training is missing the kinesiology factors and must be updated for people to recognize social engineering beyond phish clicks to help ensure no threat of this level ever faces our earth or species again.

As Bitcoin can emit the equivalent of 2,099,993.63 Hiroshima bombs I am classifying it as a CyberAtomic which must be shut down immediately.

References

1. IEEE & Oak Ridge National Laboratory, "Towards malware detection via CPU power consumption," Oak Ridge National Laboratory. https://www.ornl.gov/publication/towards-malware-detection-cpu-power-consumption-data-collection-design-and-analytics
2. MCSI Library, "Malware indicators," Cybrary, https://library.mosse-institute.com/articles/2023/07/malware-indicators.html
3. Geekscomputerrepairservices, "Computer forensics standard," High CPU usage during system idle periods. https://geekscomputerrepairservices.com.au/signs-of-a-virus-high-cpu-usage-when-system-is-idle/
4. Practical Security Analytics LLC, "Threat hunting with file entropy," https://practicalsecurityanalytics.com/file-entropy/
5. MDPI, "Encryption techniques commonly employed in ransomware," High-entropy block detection methodologies. https://www.mdpi.com/1424-8220/24/5/1446
6. Shannon, C. E. (1948). A mathematical theory of communication. Bell System Technical Journal, 27(3), 379–423. https://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf
7. Cover, T. M., & Thomas, J. A. (2006). Elements of information theory (2nd ed.). Wiley. https://onlinelibrary.wiley.com/doi/book/10.1002/047174882X
8. Lyda, R., & Hamrock, J. (2007). Using entropy analysis to find encrypted and packed malware. IEEE Security & Privacy, 5(2), 40–45. https://ieeexplore.ieee.org/document/4140989
9. Gittins, Z., et al. (2020). Malware persistence mechanisms. Procedia Computer Science, 176, 88–97. https://www.researchgate.net/publication/346066615_Malware_Persistence_Mechanisms
10. [10] MITRE ATT&CK. (2023). Persistence, Tactic TA0003. https://attack.mitre.org/tactics/TA0003/
11. Kaal, W. A., & Vermeulen, E. P. (2018). Bitcoin and the rise of decentralized autonomous organizations. Journal of Organization Design, 7(11), 1–16. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082911
12. Ekblaw, A., & Barabas, C. Bitcoin and the myth of decentralization: Socio-technical proposals for restoring network integrity. https://www.semanticscholar.org/paper/Bitcoin-and-the-Myth-of-Decentralization%3A-Proposals-Ekblaw-Barabas/74311a0d50f2870239365bfbd09a0e4615733fdf
13. [5] Park, S., et al. (2019). [Blockchain decentralization study]. Referenced in: Regulation, corruption, and decentralized autonomous organizations. Organization Science, 35(2), 1–25 https://pubsonline.informs.org/doi/10.1287/orsc.2023.18467
14. NIST. (2015). FIPS PUB 180-4: Secure hash standard (SHS). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
15. Bitcoin Wiki. (n.d.). Block hashing algorithm. https://en.bitcoin.it/wiki/Block_hashing_algorithm
16. CryptoSlate. (2025). Bitcoin mining hashrate. https://cryptoslate.com/cryptos/bitcoin/
17. [1] Hashrate Index. (2023). Bitcoin hashrate: A comprehensive guide. https://hashrateindex.com/blog/bitcoin-hashrate-a-comprehensive-guide/
18. The Bitcoin Manual. (2025). Bitcoin hashrate reaches 1 zetahash. https://thebitcoinmanual.com/articles/btc-hashrate-1-zetahash/
19. Vopson, M. M. (2019). The mass-energy-information equivalence principle. *AIP Advances*, 9(8), 085014. https://doi.org/10.1063/1.5123794
20. Walker, J. (2026). The Infoton: A Fundamental Particle of Information Energy. *Januarian Physics* https://zenodo.org/records/18210355
21. Landauer, R. (1961). Irreversibility and heat generation in the computing process. *IBM Journal of Research and Development*, *5*(3), 183–191. https://ieeexplore.ieee.org/document/5392446

22. Einstein, A. On the electrodynamics of moving bodies. Ann. Phys. 1905, 17, 891. Available 53 online: https://users.physics.ox.ac.uk/~rtaylor/teaching/specrel.pdf.
23. Restricted Data. (2013). The Hiroshima-equivalent: A modest proposal. https://blog.nuclearsecrecy.com/2013/06/07/a-modest-proposal/
24. U.S. Securities and Exchange Commission & U.S. Commodity Futures Trading Commission. (2010). Findings regarding the market events of May 6, 2010. https://www.sec.gov/news/press/2010-100a.htm
25. Institute of Electrical and Electronics Engineers. (2019). IEEE C57.12.00-19: Standard general requirements for liquid-immersed distribution, power, and regulating transformers. IEEE.
26. National Institute of Standards and Technology. (2025). Keeping stock trades fair. https://www.nist.gov/atomic-clocks/keeping-stock-trades-fair
27. Kirilenko, A. A., Kyle, A. S., Samadi, M., & Tuzun, T. (2017). The flash crash: High-frequency trading in an electronic market. Journal of Finance, 72(3), 967–998. https://www.researchgate.net/publication/312934662_The_Flash_Crash_High_Frequency_Trading_in_an_Electronic_Market
28. Walker, J., Larson, T. Cybersecurity Mindfulness: Awareness in an AI World https://www.cybersecuritymindfulness.com/
29. IBM. (2024). IBM quantum roadmap: Delivering large-scale, fault-tolerant quantum computing. https://www.ibm.com/roadmaps/quantum/
30. Vopson, M. M. (2022). The second law of infodynamics. AIP Advances, 12(12), 125310. https://researchportal.port.ac.uk/en/publications/second-law-of-information-dynamics/
31. Bruzewicz, C. D., Chiaverini, J., Hanson, R., & Wineland, D. J. (2019). Quantum computing with trapped ions. Reviews of Modern Physics, 91(3), 035001. https://pubs.aip.org/aip/apr/article-abstract/6/2/021314/570103/Trapped-ion-quantum-computing-Progress-and?redirectedFrom=fulltext
32. Aharonov, D., & Ben-Or, M. (2008). Fault-tolerant quantum computation with constant error. SIAM Journal on Computing, 38(4), 1207-1282. https://arxiv.org/abs/quant-ph/9906129
33. Cambridge Bitcoin Electricity Consumption Index (CBECI). (2025). Bitcoin electricity consumption. University of Cambridge. https://ccaf.io/cbnsi/cbeci
34. de Vries, A. (2019). Bitcoin's energy consumption is underestimated. The Conversation. https://www.researchgate.net/publication/343402945_Bitcoin's_energy_consumption_is_underestimated_A_market_dynamics_approach
35. National Institute of Standards and Technology (NIST). (2024). NIST releases first three finalized post-quantum encryption standards. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
36. IBM. (2024). IBM quantum Heron: 156-qubit processor specifications. https://www.ibm.com/quantum/hardware
37. Google Quantum AI. (2024). Google announces Willow: Quantum chip achieves breakthrough in error correction. https://blog.google/technology/research/google-willow-quantum-chip/
38. T1598: Phishing for Information Citation: MITRE ATT&CK. (2025). "Enterprise Attack: T1598 Phishing for Information." MITRE Corporation. https://attack.mitre.org/techniques/T1598/

39. Back, A. (2024). Testimony regarding correspondence with Satoshi Nakamoto. High Court of Justice, COPA v. Wright case, February 2024.
40. White House. (2025). "Executive Order: Strategic Bitcoin Reserve." March 2025.
41. Arkham Intelligence. (2025). "Who Owns the Most Bitcoin in 2026." https://info.arkm.com/research/who-owns-the-most-bitcoin-top-btc-holders-2026
42. Back, A. (2024). Email correspondence with Satoshi Nakamoto, August 2008 - January 2009 [Court documents]. COPA v. Wright, [2024] EWHC 411 (Ch), United Kingdom High Court of Justice.
43. CCN. (2025). "What Happens If Satoshi's Bitcoin Wallet Moves? Potential Outcomes to Know." https://www.ccn.com/education/crypto/what-happens-if-satoshis-bitcoin-wallet-moves/
44. Cointelegraph. (2025). "What happens to Satoshi's 1M Bitcoin if quantum computers go live?" https://www.tradingview.com/news/cointelegraph:16fb594d6094b:0-what-happens-to-satoshi-s-1m-bitcoin-if-quantum-computers-go-live/
45. EtherWorld. (2025, August 18). 51% doomsday: The moment a single mining pool could kill Bitcoin overnight. https://etherworld.co/51-doomsday-the-moment-a-single-mining-pool-could-kill-bitcoin-overnight/
46. Blockchain Academy LLC. (2025, April 23). The growing threat: Bitcoin mining pool concentration and its risks to the ecosystem. Medium. https://medium.com/bitcoin-mining-dispatch/the-growing-threat-bitcoin-mining-pool-concentration-and-its-risks-to-the-ecosystem-fe065b6cad64
47. Crypto.News. (2025, August 14). A single pool could trigger Bitcoin's next Black Swan. https://crypto.news/a-single-pool-could-trigger-bitcoins-next-black-swan/
48. S. Securities and Exchange Commission. (1934, as amended). Employment of manipulative and deceptive devices. 17 Code of Federal Regulations § 240.10b-5. https://www.ecfr.gov/current/title-17/chapter-II/part-240/subpart-A/subject-group-ECFRbda83517ce4377f/section-240.10b-5
49. Arthur, J. N., & Delfabbro, P. (2021). The psychology of cryptocurrency trading: Risk and protective factors. Journal of Behavioral Addictions, 10(2), 201-220. https://akjournals.com/view/journals/2006/10/2/article-p201.xml
50. Anderson IA, Wood W. Habits and the electronic herd: the psychology behind social media's successes and failures. Consum Psychol Rev 2020;4:83–99
51. Schultz, W. (2016). "Dopamine reward prediction error coding." Dialogues in Clinical Neuroscience, 18(1), 23-32. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4826767/
52. Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." https://bitcoin.org/bitcoin.pdf
53. Cambridge Bitcoin Electricity Consumption Index (CBECI). (2025). "Difficulty adjustment mechanism." https://ccaf.io/cbnsi/cbeci/
54. Walker, J., Larson T. (2025). Enticement neurotransmitter: How dopamine drives addictive behaviors. Cybersecurity Mindfulness. https://www.cybersecuritymindfulness.com/
55. Fiorillo, C. D., Tobler, P. N., & Schultz, W. (2003). Discrete coding of reward probability and uncertainty by dopamine neurons. Science, 299(5614), 1898-1902. https://doi.org/10.1126/science.1077349
56. Bitcoin Core. (2025). "Difficulty adjustment." Bitcoin Developer Reference. https://developer.bitcoin.org/reference/difficulty.html
57. Bitcoin Core Repository. (2025). "pow.cpp - Difficulty calculation." GitHub. https://github.com/bitcoin/bitcoin/blob/master/src/pow.cpp
58. Van Valen, L. (1973). "A new evolutionary law." Evolutionary Theory, 1, 1-30. [Red Queen hypothesis applied to competitive escalation]
59. Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." https://bitcoin.org/bitcoin.pdf

60. Sedlmeir, J., et al. (2020). "Energy consumption of blockchain technology: Beyond myth." Business & Information Systems Engineering, 62(6), 599-608.

61. U.S. Energy Information Administration (EIA). (2024). "Tracking cryptocurrency electricity consumption." https://www.eia.gov/todayinenergy/detail.php?id=61364

62. Cambridge Bitcoin Electricity Consumption Index (CBECI). (2025). "Bitcoin mining power demand." https://ccaf.io/cbnsi/cbeci/

63. de Vries, A. (2019). "Bitcoin's energy consumption is underestimated." Joule, 3(4), 801-805.

64. CoinShares. (2025). "Bitcoin mining in 2025: The harshest profitability squeeze on record." ForkLog.

65. Masanet, E., et al. (2019). "Implausible projections overestimate near-term bitcoin CO2 emissions." Nature Climate Change, 9(9), 653-654.

66. Bitcoin Mining Costs Soar in 2025. (2025). Volity.io. https://volity.io/news/bitcoin-mining-costs-2025/

67. CoinShares. (2025). "Bitcoin mining in 2025: The harshest profitability squeeze on record." ForkLog. https://forklog.com/en/bitcoin-mining-in-2025-the-harshest-profitability-squeeze-on-record-amid-all-time-highs/

68. Canaccord Genuity. (2025). "Bitcoin mining economics and cost structure analysis." Investment Research Report.

69. Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." https://bitcoin.org/bitcoin.pdf

70. Cambridge Bitcoin Electricity Consumption Index (CBECI). (2025). "Bitcoin block production rate." https://ccaf.io/cbnsi/cbeci/

71. Nakamoto, S. (2009). "Bitcoin genesis block and early mining rewards." Bitcoin Blockchain Explorer. https://blockchain.com/

72. U.S. Energy Information Administration (EIA). (2024). "Average electricity costs for industrial mining operations." https://www.eia.gov/

73. The Real Cost of Bitcoin Mining in 2025. (2025). CompareForexBrokers. https://www.compareforexbrokers.com/us/bitcoin-mining/

74. Wurtsbaugh, W. A., et al. (2017). Great Salt Lake and the challenges of multiple beneficial uses. Water Resources Management, 31(1), 399-422.https://doi.org/10.1007/s11269-016-1420-y

75. SmartAsset. (2025). Bitcoin adoption rates by state: Where cryptocurrency is most popular – 2025 study. https://smartasset.com/data-studies/bitcoin-cryptocurrency-adoption-2025

76. CryptoSlate. (2025, March 10). Utah pivots away from state Bitcoin reserve in landmark crypto legislation. https://cryptoslate.com/utah-pivots-away-from-state-bitcoin-reserve-in-landmark-crypto-legislation/

77. Abbott, B. W., et al. (2022). Emergency measures needed to rescue Great Salt Lake from ongoing collapse. Brigham Young University, Peer-reviewed publication.https://pws.byu.edu/great-salt-lake

78. Hall, S., Blakowski, M., Hungerford, H., Crouch, S., & Fugal, A. (2024). Shrinking shores, rising risks in the Great Salt Lake. Think Global Health.https://www.thinkglobalhealth.org/article/shrinking-shores-rising-risks-great-salt-lake

79. Utah Division of Water Resources. (2025, December 22). Great Salt Lake reaches historic low. State of Utah Official Website.https://water.utah.gov/great-salt-lake-reaches-new-historic-low/

80. Utah News Dispatch. (2025, July 29). Great Salt Lake slipping back into 'scary low' water levels.https://utahnewsdispatch.com/2025/07/29/great-salt-lake-levels-scary-low-drought/

81. Bloomberg/U.S. Energy Information Administration. (2024, February 1). US Bitcoin miners use as much electricity as everyone in Utah.https://www.bloomberg.com/news/articles/2024-02-01/bitcoin-miners-in-us-consume-up-to-2-3-of-nation-s-electricity

82. U.S. Energy Information Administration (EIA). (2024). Tracking electricity consumption from U.S. cryptocurrency mining operations. U.S. Department of Energy. https://www.eia.gov/todayinenergy/detail.php?id=61364

83. MDPI. (2024). Zero-carbon development in data centers using waste heat recovery technology: A systematic review. Materials, 17(22).https://www.mdpi.com/2071-1050/17/22/10101

84. ScienceDirect. (2025). Waste heat utilization of data centers based on heat pump technology from the perspectives of supply and demand: An overview.https://www.sciencedirect.com/science/article/abs/pii/S2210670725004172

85. Equinix. (2024, June 5). What is data center heat export and how does it work? Interconnections Blog. https://blog.equinix.com/blog/2024/06/05/what-is-data-center-heat-export-and-how-does-it-work/

86. McKinsey & Company. (2020, February 7). Climate risk and decarbonization: What every mining CEO needs to know. https://smartwatermagazine.com/news/mckinsey-company/climate-risk-and-decarbonization-what-every-mining-ceo-needs-know

87. ScienceDirect. (2023, June 10). Water consumption assessment in mineral processing integrating weather information and geometallurgical modeling. https://www.sciencedirect.com/science/article/abs/pii/S0892687523001760

88. MDPI. (2025). Optimizing vegetation restoration: A comprehensive index system for reclaiming abandoned mining areas in arid regions of China. Plants, 14(1), 23.https://www.mdpi.com/2079-7737/14/1/23

89. World Resources Institute. (2025). More critical minerals mining could strain water supplies in stressed regions.https://www.wri.org/insights/critical-minerals-mining-water-impacts

90. CoinCentral. (2025, March 10). Utah passes modified blockchain bill, removes Bitcoin reserve provision.https://coincentral.com/utah-passes-modified-blockchain-bill-removes-bitcoin-reserve-provision/

91. Utah Division of Water Resources. (2022). Governor Spencer Cox closure order: Great Salt Lake basin water right applications. State of Utah Official Records.https://water.utah.gov/

92. Frontiers in Environmental Science. (2022, May 13). Effect of large-scale mining drainage on groundwater hydrogeochemical evolution in semi-arid and arid regions.https://frontiersin.org/articles/10.3389/fenvs.2022.926866/full

93. [Data Center Group. (2025, December 12). Waste heat recovery from data centers: Regulatory requirements, typical use cases and optimal planning.https://www.velasolaris.com/en/data-center-heat-reuse/

94. [Scientific Reports. (2025, November 5). Maximizing waste heat recovery from a building-integrated edge data center. Nature Publishing Group.https://www.nature.com/articles/s41598-025-22498-x

95. ASME Digital Collection. (2025, February 1). Data center waste heat reuse: An investment analysis. Journal of Engineering for Sustainable Buildings and Cities, 6(1), 011002.https://asmedigitalcollection.asme.org/sustainablebuildings/article/6/1/011002/1210426/Data-Center-Waste-Heat-Reuse-An-Investment

96. Bitcoin Wiki. (n.d.). Controlled supply. https://en.bitcoin.it/wiki/Controlled_supply

97. Lopp, J. (2022, January 19). How is the 21 million Bitcoin cap defined and enforced? https://blog.lopp.net/how-is-the-21-million-bitcoin-cap-defined-and-enforced/

98. Fidelity Digital Assets. (2025). Understanding Bitcoin and Ethereum supply. https://www.fidelitydigitalassets.com/research-and-insights/understanding-bitcoin-and-ethereum-supply

99. Unchained Capital. (n.d.). How does the bitcoin source code define its 21 million cap? https://www.unchained.com/blog/bitcoin-source-code-21-million

100. CoinGecko. (2025, July 17). What happens when all bitcoin is mined? https://www.coingecko.com/learn/what-happens-last-bitcoin-mined

101. BeInCrypto. (2025, August 16). Bitcoin in 2140: How will the network survive without subsidies? https://beincrypto.com/bitcoins-endgame-2140-how-will-network-survive/

102. EZ Blockchain. (2025, November 28). When will Bitcoin hit 21 million and what happens next? https://ezblockchain.net/article/what-happens-after-all-21-million-bitcoins-are-mined/

103. Trakx. (2025, July 30). When will the last Bitcoin be mined? https://trakx.io/resources/insights/when-will-the-last-bitcoin-be-mined/

104. CoinMarketCap/Blockchain.com. (2025). Bitcoin supply data [Chart]. blockchain data providers. [10] River. (n.d.). What will happen after all Bitcoin are mined? https://river.com/learn/what-will-happen-after-all-bitcoin-mined/

105. Stoll, C., Klaaßen, L., & Gallersdörfer, U. (2019). The carbon footprint of Bitcoin. Joule, 3(7), 1647–1661. https://www.sciencedirect.com/science/article/pii/S2542435119302557

106. U.S. Energy Information Administration (EIA). (2025). "Average electricity rates for commercial and industrial users." https://www.eia.gov/electricity/data.php

107. Cambridge Centre for Alternative Finance (CCAF). (2025). "Bitcoin Mining Network Sustainability Index: Methodology." https://ccaf.io/cbnsi/cbeci/methodology

108. ECOS Mining. (2025). "Bitcoin Mining Profitability Calculator: Complete Guide 2025." https://ecos.am/en/blog/bitcoin-mining-profitability-calculator-complete-guide-2025/

109. Thunder Said Energy. (2025). "Data Center Economics: Capex and Opex cost breakdown." https://thundersaidenergy.com/downloads/data-centers-the-economics/

110. U.S. Energy Information Administration (EIA). (2024). "Tracking cryptocurrency electricity consumption." https://www.eia.gov/todayinenergy/detail.php?id=61364

111. Bitcoin Mining in 2026: Trends and Predictions. (2024). Sazmining. https://www.sazmining.com/blog/bitcoin-mining-in-2026-trends-and-predictions

112. [CoinShares. (2025). "Bitcoin mining in 2025: the harshest profitability squeeze on record amid all-time highs." ForkLog. Building and operating a bitcoin mine typically costs $700,000–$1M per MW. https://forklog.com/en/bitcoin-mining-in-2025-the-harshest-profitability-squeeze-on-record-amid-all-time-highs/

113. MIT https://web.mit.edu/12.000/www/m2016/finalwebsite/problems/ree.html

114. International Energy Agency. (2019). Bitcoin energy use: Mined the gap – Analy-sis. https://www.iea.org/commentaries/bitcoin-energy-use-mined-the-gap

115. CoinLaw. (2025). Bitcoin energy consumption statistics 2025: Efficiency, regulation & green tech. https://coinlaw.io/bitcoin-energy-consumption-statistics/

116. Bitdeer. (n.d.). How to manage electricity costs when mining bitcoin. https://www.bitdeer.com/learn/how-to-manage-electricity-costs-when-mining-bitcoin

117. Digiconomist. (2025, June 2). Bitcoin energy consumption in-dex. https://digiconomist.net/bitcoin-energy-consumption

118. Reddy, C. K. K., Kaza, V. S., Madana Mohana, R., Alamer, A., Alam, S., Mohammed, S., Basudan, S., & Sheneamer, A. (2024). Detecting and forecasting cryptojacking attack trends in Internet of Things and Wireless Sensor Networks devices. PeerJ Computer Science, 10, e2491. https://peerj.com/articles/cs-2491/

119. Mannella, L., Canavese, D., & Regano, L. (2024). Detecting cryptomining traffic in IoT networks. In 2024 9th International Conference on Smart and Sustainable Technologies (SpliTech) (pp. 1-6). IEEE. https://www.researchgate.net/publication/380193014_Detecting_Cryptomining_Traffic_in_IoT_Networks

120. Khan, R., Bhuiyan, M. Z. A., & Bhuiyan, Z. A. (2022). Research on monitoring technology of power stealing behavior in bitcoin mining based on analyzing electric energy data. Sustainable Energy Technologies and Assessments, 52, 102118. https://ui.adsabs.harvard.edu/abs/2022EnRep...8.1183K/abstract

121. Olushola, A., & Meenakshi, S. P. (2025). Cybersecurity crimes in cryptocurrency exchanges (2009–2024) and emerging quantum threats: The largest unified dataset of CEX and DEX incidents. Frontiers in Blockchain, 8, 1713637. https://colab.ws/articles/10.3389%2Ffbloc.2025.1713637

122. U.S. Energy Information Administration (EIA). (2024). Tracking electricity consumption from U.S. cryptocurrency mining operations. U.S. Department of Energy. https://www.eia.gov/todayinenergy/detail.php?id=61364

123. Gajdos, M., Sysala, T., Kusek, M., Ondracek, J., Novotny, M., & Smrz, P. (2019). How to detect cryptocurrency miners? By traffic forensics! Digital Investigation, 30, 101-110. https://www.researchgate.net/publication/335352428_How_to_detect_cryptocurrency_miners_By_traffic_forensics

Funding

This research received no external funding.

Conflicts of Interest

The author teaches Cybersecurity Mindfulness. A new cybersecurity methodology which teaches neuroscience, & kinesiology to identify and train against social engineering and quantum cybersecurity threats.

Endorsements

The Author January Walker January Walker (UP-UT-CD4) received endorsement from American Blockchain PAC alongside incumbents Sen. Mike Crapo (R-ID), Rep. Tom Emmer (R-FL-CD6), Rep. Ro Khanna (D-CA-CD17), Sen. Rand Paul (R-KY), Rep. Maria Salazar (R-FL-CD27), Rep. David Schweikert (R-AZ-CD6), Rep. Darren Soto (D-FL-CD9), Rep. Ritchie Torres (D-NY-CD15), Sen. Ron Wyden (D-OR) and candidates Maxwell Alejandro Frost (D-FL-CD10), Tom Kean, Jr. (R–NJ-CD7), Blake Masters (R-AZ-Senate), Frank Pallotta (R-NJ-CD5).