https://doi.org/10.64142/jeai.1.1.17

Journal of Engineering and Artificial Intelligence

Research Article

JEAI-25-17

Quantum Computation: An Analytical Rebuttal

Craig S Wright[*]

Department of Computer Science, University of Exeter Ltd, Exeter, UK

[*]**Corresponding author:** Craig S Wright, Department of Computer Science, University of Exeter Ltd, Exeter, UK, E-mail: craig@rcjbr.org

Received date: June 19, 2025; **Accepted date:** June 27, 2025; **Published date:** July 19, 2025

Citation: Wright CS (2025) Quantum Computation: An Analytical Rebuttal. J Eng Artif Intell Vol.1 No.1: 17.

Abstract

Quantum computing is widely portrayed as a revolutionary technological paradigm, promising exponential speedups and unprecedented computational capabilities through the manipulation of quantum superposition, entanglement and interference. This paper presents a com- prehensive and interdisciplinary refutation of such claims, demonstrating that the prevailing narrative is mathematically incoherent, physically implausible, economically irrational and politically constructed. Beginning with a rigorous critique of the misinterpretation of quantum states as parallel classical processes, we show that superposition and entanglement do not provide the kind of computational multiplicity often claimed. We examine the hard limits imposed by decoherence, error correction overhead and thermodynamic constraints, revealing that scalable, fault-tolerant quantum computation remains physically infeasible under any realistic engineering regime. We further demonstrate that quantum computing introduces no new class of computable functions and remains firmly within the boundaries of the Church–Turing thesis. Economically, we analyse the high costs and narrow applicability of proposed quantum advantages, concluding that even where theoretical speedups exist, the resource overhead renders them impractical. Finally, we dissect the political economy of quantum computing as a form of security theatre, wherein opaque scientific discourse is exploited to secure funding, generate institutional rents and sustain a techno-political myth. This paper reasserts the necessity of epistemic rigour, economic rationality and physical realism in evaluating emerging technologies and argues that the current trajectory of quantum computing investment constitutes a paradigmatic case of institutionalised overpromise

Keywords: Quantum computing critique; Church turing thesis; Quantum error correction; Superposition and entanglement; Decoherence and scalability; Thermodynamic constraints; Security theatre and techno-politics

Introduction

Quantum computing has increasingly been heralded as the future paradigm of high-performance computation, promising dramatic improvements through quantum phenomena such as superposition, entanglement and interference. The dominant narrative suggests that quantum computing will inherently enable exponential speedups, transform numerous computational domains and reshape economic landscapes. However, beneath this prevalent optimism lies a deeply embedded and systematic misunderstanding of the fundamental physics, mathematical structures, practical engineering challenges and economic realities underpinning quantum information processing. This paper rigorously deconstructs and critically rebuts these widespread claims, providing a comprehensive analysis of the inherent logical, mathematical and physical inconsistencies inherent to the standard quantum computing narrative.

This critical reevaluation is not merely academic; it has substantial policy and strategic im- plications. In an environment increasingly dominated by techno-nationalism and performative innovation, the allocation of state and private capital towards quantum initiatives must be subjected to the same analytical scrutiny applied to conventional economic and technological projects.

The scientific and engineering community bears a particular responsibility to resist the temptations of rent-seeking and rhetorical inflation, particularly when the stakes involve billions in public funds and the strategic misdirection of national research priorities.

Moreover, this paper contributes to a broader intellectual realignment an insistence on epistemic clarity, economic realism and physical feasibility in the evaluation of emerging technologies. It represents an explicit rejection of the post-truth technophilic rhetoric wherein mathematical formalism is mystified, physical limitations are abstracted away and economic costs are buried under speculative future gains. It challenges the use of complexity as a political and economic shield against accountability and proposes instead a return to sober, cross-disciplinary rationalism.

We will demonstrate throughout that the implications of this critique are not limited to quantum computing alone but resonate across a spectrum of modern technological promises. Whether in artificial intelligence, blockchain or green energy, a recurrent theme has emerged: The weaponisation of complexity to manufacture consent and extract resources under conditions of informational asymmetry. Quantum computing is perhaps the most extreme instantiation of this pattern wherein a field's opacity, rather than its productivity, becomes the primary driver of its funding.

The structure of this paper reflects this comprehensive scope. Section 1 initiates the analysis with a rigorous critique of superposition and entanglement and their widespread misinterpretation as mechanisms of classical parallelism. Section 2 addresses the profound scaling limitations imposed by decoherence and environmental coupling. Section 3 explores the logical impossibilities embedded in the no-cloning theorem and their computational ramifications. Section 4 deconstructs the myth of exponential speedup through detailed scrutiny of quantum algorithms. Section 5 imposes a thermodynamic lens on the costs of coherence, measurement and error correction. Section 6 situates quantum computation within classical complexity classes and denies it the status of ex- tending the boundaries of computability. Section 7 compares theoretical models against physical implementation constraints in detail. Section 8 exposes the economic irrationality of real-world quantum computing investments. Section 9 evaluates the political economy of quantum computing as a case study in security theatre, institutional capture and the FUD cycle.

This paper thus sets a new standard for evaluating quantum computing claims not merely within physics or computer science, but within the broader domains of economic policy, technological governance and political accountability. It does not call for an end to research in quantum foundations or coherent state manipulation; rather, it demands the disaggregation of foundational physics from overstated economic projections and politically expedient myths.

Quantum mechanics remains one of the most precise, predictive and profound theories in physics. But quantum computing, as currently constructed, is not an extension of that theoretical integrity it is a speculative structure built atop abstraction, supported by fiscal momentum and political symbolism rather than engineering feasibility or economic justification. To continue funding it without rigorous reevaluation is to indulge in a form of technocratic mysticism unbecoming of the rational principles that once governed scientific advancement.

This work stands as both a diagnosis and a corrective. It reclaims the integrity of scientific analysis against its strategic instrumentalisation. It restores computability to its formal bounds. It anchors engineering in physical realism. It reasserts economic discipline where narrative speculation has usurped constraint. And above all, it imposes clarity where confusion has been weaponised for funding. The age of quantum mythology must end and, in its place, we must restore the sober, interdisciplinary realism that alone preserves the legitimacy of science in public life.

Misuse of Superposition and Entanglement

The prevalent interpretation of quantum computing as harnessing parallelism through quantum superposition fundamentally misrepresents the rigorous physics and mathematics underpinning quantum mechanics. The quantum state of an *n*-qubit register is described within an exponential dimensional Hilbert space as:

$$|\psi\rangle = \sum_{x=0}^{2^n-1} \alpha_x |x\rangle, \quad \sum_{x=0}^{2^n-1} |\alpha_x|^2 = 1, \qquad (1)$$

where each amplitude αx encodes probability information. Yet, this superposition does not imply simultaneous classical computations. The quantum state is fundamentally indivisible, a single vector undergoing linear evolution governed strictly by the Schrodinger equation:

$$i\hbar \frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle, \qquad (2)$$

where the Hamiltonian operator H dictates deterministic, norm-preserving transformations. Claims of inherent computational parallelism arise from an incorrect analogy between abstract mathematical linearity and physical computational processes [1].

Quantum computation manipulates probability amplitudes rather than discrete logical values; computational tasks rely solely upon engineered interference patterns among amplitudes, rather than direct parallel evaluations of distinct computational branches. Quantum algorithms, such as Grover's search, explicitly illustrate this through controlled unitary evolutions, *e.g.*,

$$U_{\text{Grover}} = (2|\psi\rangle\langle\psi| - I)O_f \qquad (3)$$

where O_f is the oracle embedding the solution condition and interference selectively amplifies amplitude probabilities. Grover's algorithm offers quadratic improvement, $O(\sqrt{N})$ explicitly demonstrating the limited computational advantage even when harnessing quantum interference [2]. This refutes simplistic interpretations equating amplitude manipulation with classical parallelism.

Measurement, defined rigorously through the Born rule, fundamentally limits information extraction to a single outcome per quantum run:

$$P(x) = |\langle x|\psi\rangle|^2 = |\alpha_x|^2. \qquad (4)$$

The assertion that superposition alone provides direct computational access to multiple results simultaneously collapses under this rigorous constraint. The quantum measurement process irreversibly collapses the superposition, discarding all other encoded possibilities [3]. Any computational strategy relying on measurement must repeat the process extensively, reintroducing classical computational overheads.

The inaccessibility of the full state vector is further underlined by the no-cloning theorem:

$$\nexists U: \quad U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle \quad \forall|\psi\rangle, \qquad (5)$$

which precludes non-destructive replication of arbitrary quantum states [4]. Quantum algorithms thus intrinsically embed probabilistic verification methods; correctness emerges statistically, not deterministically.

Entanglement is similarly misconstrued. A prototypical maximally entangled Bell state:

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \qquad (6)$$

yields strong quantum correlations. Yet, the reduced density matrix yields strong quantum correlations. Yet, the reduced density matrix obtained by tracing out one subsystem explicitly illustrates maximal mixedness:

$$\rho_A = \mathrm{Tr}_B(|\Phi^+\rangle\langle\Phi^+|) = \frac{I}{2}. \qquad (7)$$

This confirms the absence of independently accessible computational resources within entanglement. The state ρA has maximal von Neumann entropy:

$$S(\rho_A) = -\mathrm{Tr}(\rho_A \log \rho_A) = \log 2, \qquad (8)$$

indicating total uncertainty when measured locally. The entanglement present does not offer local computational advantages but strictly encodes nonlocal correlations. These correlations, characterized rigorously by Bell inequalities, are statistical phenomena manifesting solely upon joint measurement. Thus, entanglement provides no direct classical parallelism or immediate computational gain; its utility in algorithms arises exclusively through carefully choreographed nonlocal interference.

Non-classical correlations exploited by quantum protocols such as quantum teleportation, superdense coding or certain cryptographic primitives (*e.g.*, BB84) rely fundamentally upon these joint statistical outcomes rather than inherent parallel computational capabilities. The quantum teleportation protocol, for example, transmits quantum states utilizing a Bell pair and classical communication:

$$|\psi\rangle_{\text{in}} \otimes |\Phi^+\rangle_{AB} \to \frac{1}{2}\sum_{i=0}^{3}(\sigma_i|\psi\rangle_B)|\Phi_i\rangle_A, \qquad (9)$$

where $\{\sigma_i\}$ are the Pauli matrices and $\{|\Phi_i\rangle\}$ form a Bell basis. However, this explicitly depends on classical communication to complete the protocol. The entanglement alone does not perform computational operations, instead enabling correlations to transfer quantum information once supplemented by classical information channels. This precise mathematical structure underscores the limited utility of entanglement in standalone computational tasks without classical coordination.

Furthermore, the potential computational benefits of quantum algorithms rely critically on physically realizable and computationally tractable quantum states and operations. Quantum state preparation and unitary evolution must contend rigorously with the limits imposed by precision and error propagation. Quantum amplitudes are continuous complex numbers, often requiring irrational values for ideal transformations. Yet physical implementation invariably demands rational approximations, governed rigorously by the Solovay–Kitaev theorem:

$$||U - U_{\text{approx}}|| \leq C \log^c(1/\epsilon), \qquad (10)$$

for some constants C, c > 0. Achieving approximation accuracy ϵ thus involves significant computational overhead, scaling polynomially yet substantially limiting accessible quantum states and gates to a strictly finite-precision computational domain.

Quantum Error Correction (QEC), central to maintaining quantum coherence, further emphasizes the fundamental constraints. Quantum stabilizer codes encode logical qubits into multi-qubit entangled states:

$$|\psi_L\rangle \mapsto |\psi_{\text{enc}}\rangle = \prod_i (I + S_i)|0\rangle^{\otimes n}, \qquad (11)$$

where $\{S_i\}$ form the stabilizer group. Crucially, QEC respects the no-cloning theorem, encoding quantum information non-locally without producing independent copies. These encoding permits syndrome measurements without collapsing logical qubit information, allowing error correction at the substantial cost of increased physical resources. Achieving fault tolerance, characterized by the quantum threshold theorem:

$$p_{\text{error}} < p_{\text{threshold}} \approx 10^{-4} \text{ to } 10^{-2}, \qquad (12)$$

demands near-perfect physical qubits and highly accurate gates, significantly raising practical implementation barriers.

Ultimately, quantum computation's purported computational advantages hinge on mathematically structured interference within physically realizable constraints. Hilbert space's exponential dimensionality does not equate to freely exploitable computational resources. Practical quantum states produced by efficient quantum circuits occupy an exponentially smaller subspace, governed by stringent physical constraints on coherence, gate fidelity and finite precision. Invoking theoretical infinity in Hilbert space dimensions as computationally meaningful is an untenable conflation of mathematical abstraction and physical reality.

Thus, rigorous analysis dismantles claims that quantum superposition and entanglement inherently provide exponential computational speedups. Quantum computing exploits intricate interference and correlations within strictly enforced mathematical, physical and computational limitations, dramatically narrowing its scope and practical viability beyond highly specialized algorithmic contexts.

The Scaling Problem: Decoherence

Quantum computing's scalability critically hinges upon preserving coherence across increasingly large quantum registers. However, the physical reality of decoherence severely constrains scalability, as increasing the number of qubits exponentially amplifies environmental interactions, drastically limiting coherent quantum evolution.

Decoherence emerges rigorously within the formalism of open quantum systems, represented by the density matrix:

$$\rho = |\psi\rangle\langle\psi|. \qquad (13)$$

Real quantum systems, inevitably interacting with their environments, rapidly transition to mixed states:

$$\rho' = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad \sum_i p_i = 1, \qquad (14)$$

where coherence between states deteriorates due to uncontrolled interactions.

The evolution of open quantum systems is precisely captured by the Lindblad master equation:

$$\frac{d\rho}{dt} = -\frac{i}{\hbar}[H,\rho] + \sum_k \left(L_k \rho L_k^\dagger - \frac{1}{2}\{L_k^\dagger L_k, \rho\} \right), \qquad (15)$$

where L_k operators define environmental coupling channels [5]. These coupling channels cause exponential decay of coherence times as qubit arrays scale.

Explicitly, coherence decay is governed by the relation:

$$\rho_{ij}(t) = \rho_{ij}(0)e^{-t/T_2}, \quad (i \neq j), \qquad (16)$$

with T_2 coherence time drastically decreasing as qubit number increases due to cumulative environmental coupling.

Given independent decoherence channels, the success probability of maintaining coherence across n qubits scales exponentially as:

$$P_{\text{success}} = (1 - p)^n \approx e^{-np}, \qquad (17)$$

where p is the single-qubit error probability per operation. Thus, coherence rapidly diminishes, making coherent computation practically impossible at scale.

Quantum Error Correction (QEC), though theoretically elegant, attempts to mitigate these effects through encoding logical qubits across multiple physical qubits. Surface codes, among the most efficient stabilizer codes, yield logical error rates:

$$P_L \sim (p/p_{\text{threshold}})^{(L+1)/2}, \qquad (18)$$

where $p_{\text{threshold}} \approx 10^{-2}$–$10^{-4}$ [6]. However, achieving such thresholds requires experimentally unrealistic fidelity levels in large qubit arrays.

Thermal environments further amplify decoherence through the Gibbs distribution:

https://doi.org/10.64142/jeai.1.1.17

$$\rho_{\text{thermal}} = \frac{e^{-\beta H}}{\text{Tr}(e^{-\beta H})}, \quad \beta = \frac{1}{k_B T}, \tag{19}$$

exponentially degrading coherence as system size grows.

Additionally, residual qubit-qubit interactions create significant cross-couplings described by the Hamiltonian:

$$H = \frac{\hbar\omega}{2} \sum_i \sigma_z^{(i)} + \sum_{i<j} J_{ij} \sigma_z^{(i)} \sigma_z^{(j)}, \tag{20}$$

leading to unintended entanglement and further coherence loss at rates increasing combinationally with qubit number.

Gate operations also introduce errors, with unitary transformations defined by:

$$U_{\text{gate}} = e^{-iH_{\text{gate}}t/\hbar}. \tag{21}$$

Each operation carries inherent error ϵ, scaling linearly with qubit number n:

$$F = 1 - \epsilon, \quad \epsilon \propto n, \tag{22}$$

drastically reducing algorithmic fidelity for large circuits.

Repeated gate operations required in algorithms exponentially compound decoherence:

$$P_{\text{algorithm}} = (1-\epsilon)^N \approx e^{-N\epsilon}, \quad \epsilon \propto n, \tag{23}$$

leading to exponential decay in computational reliability.

Ultimately, decoherence imposes intrinsic exponential limits to quantum scalability. Maintaining coherence for large-scale quantum registers demands precision exponentially beyond current experimental capabilities, fundamentally restricting practical quantum computing.

Logical Impasse: No-Cloning Theorem and Computation

The No-Cloning theorem, first articulated by Wootters and Zurek, rigorously constrains quantum information processing, prohibiting duplication of arbitrary quantum states. Formally, this theorem states explicitly that no unitary transformation U can perform the mapping:

$$U(|\psi\rangle \otimes |e\rangle) \rightarrow |\psi\rangle \otimes |\psi\rangle, \tag{24}$$

for all unknown states |ψ⟩, where |e⟩ is some fixed initial ancillary state [20] [4]. This deceptively simple statement holds profound computational consequences, as it underpins critical restrictions in quantum algorithm design, repeatability and verification.

Quantum computation's reliance on unitary evolution:

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle, \quad U^\dagger(t)U(t) = I, \tag{25}$$

implies reversibility but crucially does not imply replicability. Classical computing achieves repeatability through unlimited fan-out operations, permitting unlimited verification and redundancy. Quantum states, however, intrinsically lack such replicability due to linearity of unitary transformations.

To illustrate, suppose hypothetically one tries to clone an arbitrary superposition state:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1. \tag{26}$$

The required cloning transformation must act linearly and thus be uniquely defined by its action on basis states:

$$|0\rangle|e\rangle \rightarrow |0\rangle|0\rangle, \quad |1\rangle|e\rangle \rightarrow |1\rangle|1\rangle. \tag{27}$$

Yet, applying linearity explicitly, we observe:

$$|\psi\rangle|e\rangle = (\alpha|0\rangle + \beta|1\rangle)|e\rangle \rightarrow \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle. \tag{28}$$

True cloning, however, demands producing:

$$|\psi\rangle|\psi\rangle = (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) = \alpha^2|00\rangle + \alpha\beta|01\rangle + \beta\alpha|10\rangle + \beta^2|11\rangle, \tag{29}$$

which clearly contradicts the linear transformation outcome in (28). This contradiction rigorously proves the theorem.

The computational implications are severe. First, quantum computations cannot use classical style redundancy. Classical computations routinely duplicate intermediate results, ensuring independent verification and reliable intermediate storage. Quantum information processing loses this vital tool entirely.

Second, consider error correction strategies in quantum computing, specifically stabilizer codes, represented mathematically by the stabilizer group S:

$$\mathcal{S} = \{S_i \mid S_i|\psi_{\text{enc}}\rangle = |\psi_{\text{enc}}\rangle\}. \tag{30}$$

These codes circumvent direct cloning by encoding quantum states non-locally into entangled states across multiple qubits, allowing syndrome measurements without direct copying. Yet, this indirect redundancy significantly increases complexity and requires substantial overhead:

https://doi.org/10.64142/jeai.1.1.17

$$|\psi_{\text{enc}}\rangle = \prod_i (I + S_i)|0\rangle^{\otimes n}, \qquad (31)$$

with n ≫ 1, creating an exponential demand on physical qubit resources.

Third, this theorem sharply restricts verification and repeatability. Quantum computation fundamentally relies upon probabilistic verification through repeated state preparations rather than deterministic state verification. Unlike classical computations verifiable through exact state copies quantum verification relies on repeated executions:

$$P_{\text{verify}} \approx 1 - (1 - p_{\text{success}})^N, \qquad (32)$$

with N trials needed to achieve high confidence. Consequently, quantum computation must introduce significant overhead in both computational resources and runtime.

Further consequences arise explicitly in algorithmic complexity. Fault-tolerant quantum computation necessitates redundant quantum states protected by stabilizer codes or similar constructs, with each logical qubit requiring many physical qubits. Surface codes, for example, demand over-head scaling as:

$$n_{\text{physical}} \sim O(d^2), \quad d \propto \log(1/p_{\text{logical}}), \qquad (33)$$

where logical error rates p_{logical} exponentially depend on physical gate fidelities.

Moreover, quantum cryptographic protocols, including Quantum Key Distribution (QKD), explicitly leverage the no-cloning principle as a security resource. Security proofs, for instance in BB84, derive directly from the impossibility of perfectly cloning unknown quantum states. Eve's cloning attempt introduces detectable errors, mathematically bounded by quantum distinguishability relations:

$$P_{\text{distinguish}} \leq \frac{1}{2}(1 + \sqrt{1 - |\langle\psi|\phi\rangle|^2}), \qquad (34)$$

demonstrating mathematically provable security reliant explicitly on cloning impossibility.

Additionally, the impossibility of cloning restricts quantum network scalability. Quantum repeaters, necessary for scalable quantum communication, cannot amplify quantum signals like classical repeaters, explicitly because amplification requires state copying. Quantum repeaters thus rely heavily on entanglement distribution and purification, which are significantly resource-intensive processes mathematically governed by complex entanglement distillation protocols.

Finally, the fundamental impossibility of quantum fan-out gates places stringent limitations on quantum algorithm design. Unlike classical logic gates allowing multiple fan-outs to independent computational pathways, quantum gates:

$$U|x\rangle|y\rangle \neq |x\rangle|f(x) \oplus y\rangle, \qquad (35)$$

for arbitrary duplication of $|x\rangle$, explicitly preclude such operations. Quantum computations remain restricted to linear transformations, dramatically limiting their computational architectures.

In summary, the no-cloning theorem rigorously establishes fundamental computational restrictions unique to quantum information processing. Quantum algorithms cannot rely upon redundancy, independent verification or deterministic repeatability inherent to classical computation. Error correction and verification procedures inherently demand substantial computational over- head, profoundly limiting scalability and practical viability. These rigorous constraints underscore profound logical impasses intrinsic to quantum computational frameworks, fundamentally distinguishing quantum information processing from classical computing paradigms.

The Myth of Exponential Parallelism

The narrative frequently propagated around quantum computation that quantum superposition enables exponential parallelism rests fundamentally on a misunderstanding of quantum algorithm structures. This misconception becomes particularly evident through careful analysis of canonical quantum algorithms, notably Grover's search algorithm and Shor's factoring algorithm.

Quantum superposition describes a state within an exponentially large Hilbert space, typically denoted as:

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle, \qquad (36)$$

leading some to claim erroneously that all 2^n computations are performed simultaneously. However, the operational reality is fundamentally different.

Grover's algorithm provides a quintessential example. Designed to search an unsorted database of N = 2^n items, Grover's oracle O_f marks one solution state $|x_0\rangle$:

$$O_f|x\rangle = (-1)^{f(x)}|x\rangle, \quad f(x_0) = 1, \quad f(x \neq x_0) = 0. \qquad (37)$$

The Grover iteration operator explicitly includes amplitude inversion about the mean:

$$G = (2|\psi\rangle\langle\psi| - I)O_f, \tag{38}$$

repeated approximately $\frac{\pi}{4}\sqrt{N}$ times, achieving amplitude amplification. Final measurement yields the solution with probability approaching unity:

$$P_{\text{success}} \approx \sin^2\left((2m+1)\frac{\theta}{2}\right), \quad \theta = 2\arcsin\frac{1}{\sqrt{N}}. \tag{39}$$

The quantum advantage of Grover's algorithm, however, is explicitly quadratic rather than exponential scaling as O(√N) versus classical O(N). This quadratic improvement clearly disproves

assertions of exponential computational parallelism. Critically, the algorithm does not simultaneously "evaluate" all inputs; rather, it precisely manipulates amplitude interference structures within a single quantum state to selectively amplify solution probabilities.

Shor's algorithm provides another commonly misrepresented example. Its objective is to factor integers by reducing the problem to period-finding *via* quantum Fourier transform (QFT). The critical quantum step involves preparing a superposition state:

$$|\psi\rangle = \frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x\rangle|a^x \mod N\rangle, \tag{40}$$

where q = 2^n is chosen sufficiently large relative to integer N to ensure accurate periodicity encoding. The quantum Fourier transform then produces constructive interference peaks corresponding to multiples of the inverse period:

$$\text{QFT}_q|x\rangle = \frac{1}{\sqrt{q}}\sum_{y=0}^{q-1}e^{2\pi ixy/q}|y\rangle \tag{41}$$

A measurement of this transformed state yields an outcome close to a multiple of q/r (where r is the period), enabling efficient classical post-processing *via* continued fraction expansions to extract r and subsequently factor N. Explicitly, the success probability of obtaining a useful measurement outcome is bounded by:

$$P_{\text{success}} \geq \frac{4}{\pi^2} \approx 0.405. \tag{42}$$

Again, Shor's algorithm relies explicitly on interference within amplitude distributions rather than performing exponential parallel evaluations. The computational complexity, rigorously analyzed, scales polynomially with input size:

$$O((\log N)^3), \tag{43}$$

rather than exponentially. The claimed exponential advantage over classical factoring algorithms is true only relative to the best-known classical algorithms, but the quantum mechanism fundamentally involves structured interference not parallel classical computations.

This fundamental misconception arises from inaccurately comparing quantum computational models to classical parallel processing. Classical parallel computing explicitly executes separate computational threads independently, each yielding distinct, fully retrievable outputs simultaneously. Quantum computation, governed strictly by unitary evolution U , linearly transforms amplitudes of a single state vector:

$$U: \quad |\psi_{\text{in}}\rangle \to |\psi_{\text{out}}\rangle, \quad U^\dagger U = I. \tag{44}$$

Measurement collapses the state to a single classical outcome with probabilities dictated by the Born rule:

$$P(x) = |\langle x|\psi\rangle|^2. \tag{45}$$

Thus, quantum algorithms must carefully engineer interference patterns to ensure that measurement outcomes yield the desired solution efficiently. The exponential dimensionality of the quantum Hilbert space is a purely mathematical abstraction it is not a practically accessible computational resource. Physically realizable quantum computations remain strictly constrained by measurement, coherence times and error rates.

The critical distinction between quantum and classical parallelism further emerges explicitly from Holevo's bound. Although quantum states may encode superpositions over exponentially many states, Holevo's theorem rigorously restricts the classical information extractable from an n-qubit state to at most n classical bits:

$$\chi \leq S(\rho) - \sum_i p_i S(\rho_i) \leq n, \tag{46}$$

where χ represents accessible classical information and S(ρ) denotes von Neumann entropy.

This theorem mathematically invalidates assertions equating quantum superpositions to parallel classical computations. Quantum algorithms explicitly exploit interference patterns to indirectly gain algorithm-specific computational speedups. This indirect, structured mechanism significantly limits quantum advantages to particular algorithmic contexts, rendering general claims of exponential parallelism incorrect.

In conclusion, careful mathematical scrutiny of Grover's and Shor's algorithms demonstrates explicitly that quantum computation does not perform exponentially parallel classical computations. Instead, quantum algorithms achieve their advantages through finely-tuned interference phenomena, probability amplification and structured amplitude manipulation within stringent physical and mathematical constraints. Claims suggesting exponential quantum parallelism thus constitute fundamental misunderstandings of quantum computational mechanisms.

Thermodynamic Constraints and Information Realism

Quantum computing narratives frequently omit rigorous thermodynamic considerations, particularly those articulated explicitly by Landauer's principle and its profound implications for information processing. Landauer's principle states unequivocally that any logically irreversible manipulation of information is inevitably accompanied by an entropy increase, thereby imposing a fundamental thermodynamic cost.

Landauer's principle quantitatively asserts the minimal energy required to erase a single classical bit of information at absolute temperature T:

$$E_{\text{min}} = k_B T \ln 2, \tag{47}$$

where k_B is Boltzmann's constant [7]. While quantum computation utilizes unitary transformations, theoretically reversible and thus entropy-conserving, practical quantum computing implementations necessarily involve irreversible operations due to measurement, decoherence and error correction, all of which impose fundamental thermodynamic limitations.

Explicitly, the von Neumann entropy provides a quantum analog for thermodynamic entropy:

$$S(\rho) = -k_B \operatorname{Tr}(\rho \log \rho), \tag{48}$$

where ρ is the density matrix describing the quantum state. Any realistic quantum computation involving measurement transforms pure states into mixed states irreversibly, explicitly increasing entropy and thus necessitating energy dissipation.

Practically, quantum computation demands maintaining coherent quantum states, typically *via* thermal isolation. Yet, perfect isolation is impossible due to thermodynamic irreversibility inherent in maintaining low entropy states. The Gibbs state at equilibrium provides the explicit thermodynamic limit of maintaining coherence:

$$\rho_{\text{eq}} = \frac{e^{-\beta H}}{\operatorname{Tr}(e^{-\beta H})}, \quad \beta = \frac{1}{k_B T}. \tag{49}$$

Even minuscule coupling to thermal reservoirs causes rapid equilibration, explicitly limiting coherence times exponentially as temperature or coupling strength increases.

Quantum Error Correction (QEC), central to quantum computing viability, explicitly entails entropy increases due to continuous syndrome measurements, an inherently irreversible process. Consider a stabilizer code, described by stabilizer operators $\{S_i\}$, applied repeatedly to detect errors:

$$S_i|\psi_{\text{enc}}\rangle = \pm|\psi_{\text{enc}}\rangle. \tag{50}$$

Syndrome extraction measurements collapse superpositions irreversibly, generating entropy explicitly *via*:

$$\Delta S_{\text{measure}} \geq k_B \ln 2\, H(p), \tag{51}$$

where H(*p*) is the Shannon entropy associated with measurement outcome probabilities. This irreversible entropy generation explicitly demands energy dissipation, following Landauer's bound rigorously.

Additionally, practical quantum gates, although ideally reversible, possess finite fidelity F, causing unintended state perturbations and irreversibility:

$$F = \langle\psi_{\text{ideal}}|\rho_{\text{real}}|\psi_{\text{ideal}}\rangle \leq 1. \tag{52}$$

Finite gate fidelity introduces irreversible state entropy, explicitly bounded by the quantum Fano inequality:

$$S(\rho_{\text{real}}) \geq H(F) + (1 - F)\log(d - 1), \tag{53}$$

where d is Hilbert space dimension. These entropy increases, explicitly quantifiable, further exacerbate thermodynamic limitations.

Quantum computation also requires cooling qubits below thermal fluctuation scales to maintain coherence. The Carnot efficiency imposes fundamental lower limits on cooling power efficiency:

$$\eta_{\text{Carnot}} = 1 - \frac{T_{\text{cold}}}{T_{\text{hot}}}, \tag{54}$$

where $T_{cold} \ll T_{hot}$. Maintaining ultra-low entropy states thus explicitly demands enormous thermodynamic expenditures, exponentially escalating with system size.

Furthermore, quantum memory storage explicitly suffers thermodynamic limits. Quantum error correction codes encode logical qubits into entangled arrays of physical qubits. Consider the entanglement entropy for stabilizer codes:

$$S_A = -k_B \mathrm{Tr}(\rho_A \log \rho_A), \quad (55)$$

where ρA is a subsystem density matrix. Maintaining coherent entanglement explicitly requires energy input exceeding minimal bounds set by thermodynamics.

Explicit physical realizations, such as superconducting qubits, ion traps or spin systems, exhibit unavoidable environmental coupling rates Γ, dictated rigorously by the fluctuation-dissipation theorem:

$$S_\omega = \frac{2\hbar\omega}{1 - e^{-\hbar\omega/k_B T}}, \quad (56)$$

explicitly linking decoherence rates to thermodynamic temperature T. The quantum coherence lifetime explicitly diminishes exponentially with increasing qubit numbers due to amplified environmental coupling and irreversibility.

Consequently, the thermodynamic cost of quantum computations explicitly grows exponentially with system size and computational complexity. The total entropy production, governed explicitly by the second law of thermodynamics, satisfies:

$$\Delta S_{\text{total}} = \Delta S_{\text{system}} + \Delta S_{\text{environment}} \geq 0, \quad (57)$$

necessitating corresponding irreversible energy dissipations.

Therefore, quantum computing implementations explicitly confront fundamental thermodynamic constraints, rigorously bounded by Landauer's principle, entropy costs, cooling demands and unavoidable irreversibility. These constraints sharply restrict operational coherence, achievable fidelity, practical scalability and the genuine computational advantages of quantum systems, thus enforcing rigorous thermodynamic realism onto quantum computing narratives.

Mathematical Incoherence of "Quantum Advantage"

Claims of "quantum advantage" the assertion that quantum computing extends computational boundaries defined by classical computation often ignore fundamental mathematical and computational constraints encapsulated by the Church-Turing thesis. The Church–Turing thesis rigorously postulates that any effectively calculable function can be computed by a Turing machine. Formally, it states that no physically realizable computing device can exceed the computational power of a Turing machine in terms of computability class [8,9].

Quantum computing operates within the complexity class BQP (Bounded-error Quantum Polynomial-time), defined explicitly as:

$$\mathrm{BQP} = \{L \mid \exists \text{ quantum poly-time algorithm } A,\ \forall x \in L,\ P[A(x) = 1] \geq 2/3\}. \quad (58)$$

Critically, complexity theorists rigorously show:

$$\mathrm{BQP} \subseteq \mathrm{PSPACE}, \quad (59)$$

demonstrating explicitly that quantum computers do not transcend classical computability but are instead strictly bounded within classical complexity hierarchies.

The Church–Turing thesis explicitly implies a boundary for computability:

$$f : \mathbb{N} \to \mathbb{N}, \quad f \text{ is computable} \Leftrightarrow \exists \text{ Turing machine } M \text{ computing } f. \quad (60)$$

Quantum computing adheres strictly to these computability boundaries. No quantum algorithm can compute a non-Turing-computable function, a consequence rigorously established through quantum simulation arguments.

Specifically, quantum circuits are explicitly modeled through sequences of unitary transformations, represented mathematically as products of quantum gates drawn from a finite universal set:

$$U = U_k U_{k-1} \dots U_2 U_1, \quad U_i \in \{H, T, CNOT, \dots\}, \quad (61)$$

where each gate U_i is efficiently simulable by a classical Turing machine to arbitrary accuracy. The Solovay–Kitaev theorem rigorously ensures any quantum gate can be approximated by a finite gate set within polynomial overhead:

$$\|U - U_{\text{approx}}\| \leq \epsilon, \quad \text{with complexity} \quad O(\log^c(1/\epsilon)), \quad (62)$$

demonstrating explicitly that quantum operations provide no computability extension beyond classical models.

Quantum algorithms, such as Shor's and Grover's, offer polynomial or sub-exponential speedups over the best-known classical algorithms for specific problems. Shor's factoring algorithm, for ex- ample, provides exponential speedup relative to known classical factoring algorithms, but factoring remains strictly within the class NP ∩ co-NP, with no established super-polynomial lower bound:

$$\text{FACTORING} \in \text{NP} \cap \text{co-NP}, \quad (63)$$

explicitly showing quantum advantage remains strictly relative, not absolute.

Grover's algorithm provides at most quadratic speedup:

$$O(\sqrt{N}) \quad \text{quantum vs.} \quad O(N) \quad \text{classical}, \quad (64)$$

explicitly reaffirming quantum computing's bounded advantage. This polynomial enhancement explicitly fails to breach classical computability constraints.

Moreover, quantum algorithms require classical post-processing, strictly bounded within classical complexity classes. Shor's algorithm explicitly employs classical continued fraction expansion for period extraction:

$$\frac{s}{q} \approx \frac{k}{r}, \quad r \text{ period extracted classically}, \quad (65)$$

confirming explicitly quantum computing's inherent dependence upon classical computation.

Explicitly invoking the notion of Turing machine simulation further confirms this limitation. The quantum Church–Turing thesis, a variant rigorously established by Bernstein and Vazirani, explicitly argues:

Any quantum computation can be simulated on a probabilistic Turing machine with polynomial overhead.

This explicit constraint demonstrates that quantum computational models do not provide new classes of computability beyond classical Turing-computable functions.

Furthermore, the quantum circuit model explicitly incorporates probabilistic measurement outcomes, bounded by computational complexity constraints described by Holevo's theorem:

$$\chi \leq S(\rho) - \sum_i p_i S(\rho_i) \leq n, \quad \text{for } n\text{-qubit systems}. \quad (66)$$

Thus, quantum computational models remain strictly within classical information-theoretic limits.

Considering explicit lower bounds, rigorous results from complexity theory suggest that substantial quantum speedups relative to classical computation are exceedingly limited and context-specific. Quantum computational complexity remains strictly constrained within classical polynomial hierarchies, with explicit proven containments such as:

$$\text{BQP} \subseteq \text{PP}, \quad (67)$$

highlighting rigorous mathematical bounds constraining quantum computational advantage.

Quantum complexity theorists further conjecture that explicit quantum-classical separations remain minimal without breakthroughs in classical complexity theory. Unless proven complexity class separations emerge explicitly from classical computation theory, quantum computing's claimed "advantage" remains contextually relative rather than absolute.

In conclusion, rigorous mathematical examination explicitly demonstrates the incoherence of assertions claiming quantum computation provides novel extensions to classical computability as rigorously defined by the Church–Turing thesis. Quantum computing, bound explicitly within classical computability and complexity hierarchies, offers at best polynomially bounded algorithmic speedups for specific structured problems. Claims of unbounded "quantum advantage" thus constitute profound misunderstandings, explicitly refuted by rigorous mathematical and computational complexity analyses.

Engineering *vs.* Physics

Quantum computing narratives frequently abstract away critical real-world constraints inherent in physical implementations, including temperature, mass, decoherence, noise and interference. These simplifications produce fundamentally misleading projections, divorcing theoretical quantum algorithms from rigorous engineering realities.

The preservation of quantum coherence a fundamental prerequisite for quantum computation explicitly depends on stringent physical conditions. Quantum states used in computations require near-zero thermal fluctuations. The thermal state for a quantum system is defined rigorously by the Gibbs distribution:

$$\rho_{\text{thermal}} = \frac{e^{-\beta H}}{\text{Tr}(e^{-\beta H})}, \quad \beta = \frac{1}{k_B T}, \quad (68)$$

where T is the temperature. Achieving coherence lifetimes adequate for computation necessitates temperatures on the order of millikelvin (mK), imposing fundamental and substantial engineering challenges due to thermodynamic cooling limits described by the Carnot efficiency:

$$\eta_{\text{Carnot}} = 1 - \frac{T_{\text{cold}}}{T_{\text{hot}}}, \quad (69)$$

explicitly limiting cooling efficiency exponentially as target temperatures approach absolute zero.

Mass and physical scale represent additional fundamental engineering constraints. Quantum coherence explicitly deteriorates with increasing system size due to interaction cross-sections that scale with physical dimensions. For instance, superconducting qubits and trapped-ion systems both explicitly exhibit interaction-induced decoherence rates proportional to system scale:

$$\Gamma \propto \sigma n_{\text{env}} v_{\text{thermal}}, \quad (70)$$

where σ is interaction cross-section, n_{env} environmental particle density and v_{thermal} thermal velocity. Explicitly, as systems scale physically, decoherence increases significantly, contradicting simplified scalability assumptions in quantum computing proposals.

Real-world quantum systems explicitly suffer from physical noise, typically modeled as stochastic perturbations to idealized Hamiltonians:

$$H_{\text{real}} = H_{\text{ideal}} + \delta H(t), \quad (71)$$

where δH(t) represents environmental noise. Quantum coherence explicitly decays due to these time-dependent perturbations, described rigorously by decoherence rates derived from the fluctuation- dissipation theorem:

$$S(\omega) = \frac{2\hbar\omega}{1 - e^{-\hbar\omega/k_B T}}, \quad (72)$$

with explicit temperature dependence. Realistic quantum computing hardware thus explicitly demands unphysical suppression of noise amplitudes to maintain theoretical coherence thresholds. Physical interference from electromagnetic radiation, vibrations and mechanical instabilities explicitly further constrains coherence. Mechanical vibrations couple explicitly to quantum systems *via* interaction Hamiltonians of form:

$$H_{\text{int}} = x_{\text{sys}} F_{\text{ext}}(t), \quad (73)$$

where x_{sys} is system displacement operator and $F_{\text{ext}}(t)$ external force noise. Real quantum hardware explicitly demands mechanical isolation orders of magnitude beyond conventional engineering capabilities, severely restricting achievable coherence times.

Electromagnetic interference explicitly induces decoherence through coupling to environmental photon modes, modeled by Jaynes-Cummings-type Hamiltonians:

$$H = \frac{\hbar\omega}{2}\sigma_z + \hbar\omega_r a^\dagger a + \hbar g(\sigma_+ a + \sigma_- a^\dagger), \quad (74)$$

where g quantifies coupling strength. The explicit need for near-zero coupling (g ≈ 0) imposes stringent physical constraints incompatible with practical engineering, making scalable quantum architectures extremely fragile.

Physical qubit architectures explicitly introduce unavoidable crosstalk and inter-qubit coupling errors. For example, in superconducting qubit arrays, unintended nearest-neighbor coupling described explicitly by:

$$H_{\text{cross}} = \sum_{i \neq j} J_{ij} \sigma_z^{(i)} \sigma_z^{(j)}, \quad (75)$$

drastically reduces fidelity, limiting scalability and algorithm complexity. Physical systems explicitly impose finite minimal distances between qubits, further exacerbating these unwanted interactions.

Engineering reality explicitly contradicts theoretical assumptions regarding Quantum Error Correction (QEC). Stabilizer codes, essential for fault-tolerant quantum computation, demand physical gate fidelities explicitly above rigorous thresholds:

$$p_{\text{error}} < p_{\text{threshold}} \approx 10^{-4}. \quad (76)$$

Physically achieving such precision explicitly confronts fundamental engineering limitations in gate control electronics, quantum control pulses and coherence preservation, making practical scalability inherently challenging.

Mass and inertia explicitly impose further fundamental limits, notably in trapped-ion architectures. Ion trap stability requires precise electromagnetic confinement potentials, described explicitly by Mathieu equations governing ion trajectories:

$$\frac{d^2u}{d\tau^2} + [a_u - 2q_u \cos(2\tau)]u = 0, \quad (77)$$

where explicit stability regions impose stringent mass and frequency constraints incompatible with scaling to large qubit arrays, thereby explicitly limiting quantum register sizes.

The physical density of quantum hardware also explicitly restricts heat dissipation. Irreversible operations (such as measurement and QEC) explicitly generate heat at minimal Landauer bounds:

$$Q_{\min} = k_B T \ln 2, \qquad (78)$$

necessitating complex and large-scale cryogenic cooling systems. Such systems explicitly violate simplistic scalability assumptions, imposing exponential energy costs explicitly scaled with qubit number.

In summary, quantum computing proposals frequently abstract away fundamental physical and engineering constraints, rigorously quantified by thermodynamics, quantum coherence models and real-world interference mechanisms. Explicit analyses of temperature, mass, decoherence, noise and mechanical interference impose severe practical constraints explicitly overlooked in theoretical proposals, profoundly restricting the viability of scalable quantum computation and rendering simplified quantum computing narratives physically unrealistic.

Economic Nonsense

Quantum computing has often been heralded as revolutionary, promising dramatic breakthroughs in computational efficiency and capabilities. However, a rigorous economic analysis reveals significant practical limitations, undermining such exaggerated claims. The purported economic advantages of quantum computing primarily rest on three fundamental assumptions: (1) That quantum computers can efficiently solve computational problems significantly faster than classical counterparts; (2) that the economic cost of developing and operating quantum computing infrastructure is justifiable relative to its problem-solving capabilities; and (3) that quantum computers will scale similarly to classical computing systems.

First, consider the issue of computational speedups. Quantum algorithms such as Shor's and Grover's offer potential advantages for specific mathematical problems like factoring integers or searching databases, respectively. However, the real-world economic value of these advantages remains highly questionable. Shor's algorithm, for instance, theoretically reduces integer factorisation complexity from exponential (best known classical algorithms) to polynomial time (specifically, cubic complexity). Nevertheless, translating theoretical polynomial-time complexity to practical economic viability is problematic. Current quantum technology implementations require significant overheads in error correction and physical qubit management, substantially diluting any theoretical speedup. For instance, current experimental demonstrations are limited to very small integer factorisations, far below economically relevant scales such as those required for cryptographic key recovery: Content reference (oaicite:0) index=0.

To quantify, consider a hypothetical quantum computer constructed to break Elliptic-Curve Cryptography (ECC) utilised in cryptocurrencies like Bitcoin. Even optimistically assuming advances in quantum algorithms and infrastructure, research estimates that such a machine would require between 1 to 20 billion US dollars to operate and could feasibly crack only approximately 12 ECC private keys per year. The timeframe to reverse-engineer a single ECC key optimistically stands at around 30 days under ideal conditions: Content reference (oaicite:1) index=1. Given that any practical cryptocurrency strategy involves frequently rotating keys or utilising multi-signature schemes, such quantum-based attacks quickly become economically unviable. For in- stance, a 15-of-15 multi-signature configuration would extend the required attack duration to roughly 18 months, dramatically exceeding any practical threshold for economically justified expenditures: Content reference (oaicite:2) index = 2.

Second, the fundamental structure of quantum computing systems implies prohibitive eco- nomic costs. Quantum systems inherently require extensive infrastructure for maintaining coherence, such as ultra-cold refrigeration, precise magnetic shielding and error-correction proto- cols, vastly exceeding costs associated with classical computing systems. Furthermore, quantum hardware exhibits substantially slower processing speeds in practical tasks such as hash collisions, where classical ASIC-based systems offer orders of magnitude more efficiency. Bernstein demonstrated explicitly that quantum algorithms for hashing problems, vital for tasks such as Bitcoin mining, are not merely suboptimal but fundamentally slower than classical counter-parts: Content Reference(oaicite:3) index=3.

Third and perhaps most critically, the presumed scaling analogy between quantum and classical computing is deeply flawed. Classical computing achieved its rapid economic proliferation primarily through exponential scaling described by Moore's Law, driven by miniaturisation, energy efficiency improvements and incremental cost reductions. In stark contrast, quantum computers do not benefit similarly from scaling economies. The delicate and resource-intensive nature of quantum coherence and error correction mechanisms necessitates exponentially increasing overheads as the number of qubits grows. Thus, unlike classical computing, quantum systems will remain large-scale infrastructure projects confined to specialised data centres and governmental facilities, incapable of economic miniaturisation or widespread consumer accessibility: content reference (oaicite:4) index=4.

Further exacerbating economic concerns, there is extensive historical evidence demonstrating systemic overpromising within the quantum computing research community, driven partly by competitive funding environments. Researchers must oversell potential results and downplay uncertainties or theoretical limitations, leading to a cycle of exaggerated claims that do not materialise into economically viable products. Notably, despite decades of research and substantial funding, we have yet to see any economically significant quantum computing implementation outperform classical computing in real-world applications: Content reference (oaicite:5) index=5.

In conclusion, a detailed economic critique demonstrates that quantum computing, despite theoretical allure, offers negligible practical economic benefits for most real-world computational problems. Its substantial cost, minimal practical applicability and fundamental scalability constraints ensure quantum computing remains economically unjustified for the foreseeable future, rendering most claimed applications economically nonsensical.

Quantum Computing as Security Theatre: Funding, Fear, Uncertainty and Doubt

Introduction: The politics of quantum rhetoric

Quantum computing exemplifies the phenomenon political scientists and economists label “security theatre,” wherein a symbolic projection of security and technological superiority is strategically employed, regardless of actual efficacy. Politicians, confronting complex, esoteric technologies they scarcely comprehend, become susceptible to manipulation *via* deliberately cultivated narratives that incite Fear, Uncertainty and Doubt (FUD). These dynamic fuels excessive expenditures justified through perceived existential threats rather than tangible, demonstrable outcomes.

Economic rent-seeking and strategic manipulation

At its core, the quantum computing sector provides a paradigmatic example of classical rent- seeking as theorized by Tullock and Buchanan [10,11]. Entities seeking to secure substantial public investment propagate overstated narratives regarding quantum threats especially regarding cyber-security and cryptographic vulnerabilities to induce political urgency. In this light, investment in quantum computing becomes analogous to “economic rents,” transfers of wealth from the broader public economy to specialized research institutions and corporate entities without commensurate economic or public benefit. The economic efficiency of such investments becomes questionable, especially when examined through public-choice economic theory, which predicts inefficiencies due to information asymmetries and institutional capture [12].

The physics of fear: Misunderstanding quantum threats

From a rigorous quantum physics perspective, the practical realization of quantum technologies, particularly quantum cryptanalysis algorithms like Shor’s, remains deeply problematic. Shor’s algorithm theoretically compromises RSA encryption and Elliptic-Curve Cryptography (ECC) by reducing factoring complexity from sub-exponential to polynomial time [13]. Yet, physical limitations quantum decoherence, qubit error rates, scaling issues make real-world quantum cryptanalysis exceptionally difficult, verging on practically impossible at economically relevant scales [6]. Nevertheless, the complexity and opacity of quantum physics permit proponents to exaggerate quantum threats, generating widespread fear amongst policymakers unfamiliar with detailed scientific limitations.

Informational asymmetries and principal-agent problems

Quantum computing vividly illustrates informational asymmetries central to principal-agent theory in economics [14]. Politicians (principals), lacking quantum physics expertise, rely heavily on scientists, lobbyists and corporations (agents) whose interests may diverge sharply from public welfare. The opacity and technical complexity of quantum physics allow agents substantial leeway to inflate threats and promises selectively, securing generous funding streams disconnected from tangible results. These dynamics exemplify Akerlof’s “market for lemons,” where informational opacity systematically distorts resource allocation, promoting economically inefficient outcomes [15].

Political signalling and competitive nationalism

Quantum computing investment also functions prominently as political signalling analogous to Spence’s labour market signals demonstrating governmental technological competence and international competitiveness, independent of practical results [16]. Nation-states, driven by competitive nationalism and geopolitical rivalries (*e.g.*, between the U.S. and China), increasingly portray quantum computing as strategically indispensable. Terms such as “quantum supremacy,” coined by Preskill, have been politically co-opted into national security discourses, exacerbating competitive arms-race dynamics [17]. Yet, this competitive signalling rarely translates into genuine strategic advantages, instead perpetuating resource-intensive technological nationalism devoid of clear strategic benefit.

Quantum computing and the dynamics of security theatre

The concept of "security theatre," articulated by Schneier, provides a powerful analytical lens to critique quantum computing narratives [18]. Quantum computing initiatives symbolically project security and technological superiority without demonstrable improvements in national security or economic utility. Politicians and bureaucracies embrace quantum technology investment precisely because its complexity allows symbolic demonstrations of proactive governance. Yet, the tangible effectiveness remains negligible, mirroring historical phenomena like missile defence systems, high- energy particle physics and fusion energy fields where extensive funding has persisted largely through symbolic political efficacy rather than demonstrable economic utility.

Institutional capture and policy lock-in

Extensive quantum computing investments create powerful institutional path dependencies, aligning with theories of policy lock-in [19]. Once significant resources are committed, institutional inertia and vested interests perpetuate funding irrespective of empirical efficacy. Bureaucracies, research institutions and industries form powerful coalitions maintaining quantum computing narratives to preserve budgetary allocations, ensuring ongoing resource diversion from more empirically justified projects.

Opportunity costs and economic misallocation

Economically, quantum computing investment incurs substantial opportunity costs, diverting resources from potentially more beneficial research and technological development areas. Economic literature rigorously demonstrates how misallocation of resources *via* politically driven rather than economically justified projects diminishes overall social welfare and innovation productivity [20]. Quantum computing's substantial infrastructure costs (ultra-low temperatures, expensive error-correction methods, precise electromagnetic shielding) exacerbate its comparative inefficiency against alternative scientific and technological research programmes.

Policy recommendations: Reintroducing accountability and rationality

A rational policy response, from both economic and political perspectives, demands reintroducing critical accountability mechanisms. Robust interdisciplinary evaluation processes involving rigorous economic analysis, comprehensive peer-reviewed physical science assessments and independent oversight can mitigate the pervasive informational asymmetries. Transparent communication of quantum computing's realistic capabilities, limitations and genuine threat landscape is crucial to counteract politically induced FUD narratives and ensure economically rational resource allocation.

Conclusion: The illusion of quantum security

In summary, quantum computing epitomises modern security theatre politically effective symbolism masking scientific impracticality and economic inefficiency. Policymakers, driven by political incentives and informational asymmetries, perpetuate cycles of resource-intensive investment in quantum technologies without substantial practical benefits. A rigorous interdisciplinary critique combining political economy, advanced economic theory and rigorous quantum physics underscores the necessity of reorienting policy towards realistic assessment frameworks. Only then can policymakers effectively manage emerging technologies and avoid costly misallocations driven by fear, uncertainty and politically manufactured doubt.

Conclusion

This paper has presented a comprehensive and interdisciplinary critique of the foundational assumptions, practical viability and political economy of quantum computing. Through an integrated analysis spanning quantum physics, mathematical computability, thermodynamics, economic rationality, engineering feasibility and political theory, we have demonstrated that the dominant narrative surrounding quantum computing is not merely overstated it is structurally unsound.

We began by rigorously dismantling the core conceptual errors around superposition and entanglement. Contrary to popular belief, quantum states do not represent parallel classical computations and quantum evolution being linear, unitary and indivisible does not instantiate exponential simultaneous evaluation. Measurement collapse, the no-cloning theorem and decoherence collectively constrain the manipulation and verification of quantum information in ways that are fundamentally incompatible with the demands of scalable, fault-tolerant and economically useful computation.

The failure of quantum systems to scale coherently, thermodynamically or economically was made explicit through both theoretical modelling and reference to contemporary hardware limitations. Claims of quantum speedup were shown to be not only rare and highly problem-specific but also nullified by the massive physical overhead required to preserve fidelity, suppress noise and correct errors. From a computability-theoretic standpoint, we demonstrated that quantum computation resides strictly within the bounds of Turing computability. It does not violate, extend or challenge the Church–Turing thesis, nor does it introduce novel classes of effective calculability.

Furthermore, we have shown that even within its narrow computational niche, quantum computing's economic rationale collapses under scrutiny. The real costs of quantum hardware cryogenics, isolation, error correction, verification and energy overwhelm any theoretical performance gains. Applications such as quantum cryptanalysis are economically infeasible under realistic engineering constraints. The comparison with classical computation exposes quantum computation as both slower and costlier for nearly all relevant tasks, particularly in domains like hashing and cryptographic key reversal where classical ASICs dominate both in cost and efficiency.

Most critically, we have examined the sociopolitical structure that sustains quantum computing in the public sphere. The field functions as a form of security theatre, operating within a FUD driven funding model where the complexity of the science is exploited to secure political and institutional rents. Policymakers operating under informational asymmetry and incentivised by geopolitical signalling have become complicit in sustaining a narrative untethered from physical or economic reality. The result is a misallocation of public resources toward an initiative that serves more as political spectacle than scientific advancement.

Quantum computing, as currently promoted, represents a confluence of mathematical misinterpretation, physical abstraction, engineering fantasy, economic irrationality and political opportunism. It is a textbook example of institutionalised overpromise, sustained by a strategic interplay of opacity, symbolism and speculative futurism. The consequence is not merely a failed technology, but a distortion of the scientific process itself where demonstration yields to persuasion and funding follows fear.

This paper therefore demands a moratorium on the unfettered promotion of quantum computing as a universally transformative technology. It calls for a return to physical, mathematical and economic rigor in evaluating claims and for the reassertion of falsifiability, accountability and epistemic discipline in technological discourse. Quantum mechanics remains one of the greatest scientific achievements in human history; it does not need to be cheapened by its co-option into techno-political mythmaking.

In the final analysis, quantum computing may still yield niche, low-level scientific applications in materials simulation or quantum metrology. But it will not revolutionise computation, displace classical cryptography or redefine economic productivity. To continue asserting otherwise is not optimism it is obfuscation. It is the duty of this generation of scientists, economists and policy-makers to restore clarity where confusion has reigned and to terminate the quantum computing narrative where its theoretical integrity and practical viability no longer support its continuation. Only then can public trust in science be preserved and the future of technological investment be secured through reason, not rhetoric.

References

1. Nielsen MA, Chuang IL (2010) Quantum computation and quantum information. [Google Scholar]
2. Grover LK (1997) Quantum mechanics helps in searching for a needle in a haystack. Phys Rev Lett 79: 325-328. [Crossref], [Google Scholar]
3. Holevo AS (1973) Bounds for the quantity of information transmitted by a quantum communication channel. Probl Inf Trans 9: 177-183. [Google Scholar]
4. Wootters WK, Zurek WH (1982) A single quantum cannot be cloned. Nature 299: 802-803. [Crossref], [Google Scholar]
5. Lindblad G (1976) On the generators of quantum dynamical semigroups. Commun Math Phys 48: 119-130. [Crossref], [Google Scholar]
6. Fowler AG, Mariantoni M, Martinis JM, Cleland AN (2012) Surface codes: Towards practical large-scale quantum computation. Phys Rev A 86: 032324. [Crossref], [Google Scholar]
7. Landauer R (1961) Irreversibility and heat generation in the computing process. IBM J Res Dev 5: 183-191. [Crossref], [Google Scholar]
8. Church A (1936) An unsolvable problem of elementary number theory. Am J Math 58: 345-363. [Crossref], [Google Scholar]
9. Turing AM (1937) On computable numbers, with an application to the entscheidungsproblem. Proc Lond Math Soc 42: 230-265. [Crossref], [Google Scholar]
10. Tullock G (1967) The welfare costs of tariffs, monopolies and theft. Econ Inq 5: 224-232. [Google Scholar]

11. Buchanan JM (2008) Rent seeking and profit seeking. [Crossref], [Google Scholar]

12. Mancur O (1965) The logic of collective action: Public goods and the theory of groups. [Google Scholar]

13. Shor PW (1997) Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J Comput 26: 1484-1509.[Crossref], [Google Scholar]

14. Jensen MC, Meckling WH (1976) Theory of the firm: Managerial behavior, agency costs and ownership structure. J Financ Econ 3: 305-360. [Crossref], [Google Scholar]

15. Akerlof GA (1970) The market for “Lemons”: Quality uncertainty and the market mechanism. Q J Econ 84: 488-500. [Google Scholar]

16. Spence M (1973) Job market signaling. Q J Econ 87: 355-374. [Google Scholar]

17. Preskill J (2012) Quantum computing and the entanglement frontier. arXiv preprint. [Crossref], [Google Scholar]

18. Schneier B (2003) Beyond fear: Thinking sensibly about security in an uncertain world. Springer 181-206. [Google Scholar]

19. Pierson P (2000) Increasing returns, path dependence and the study of politics. Am Political Sci Rev 94: 251-267. [Google Scholar]

20. WJ Baumol (1990) Entrepreneurship: Productive, unproductive and destructive. J Pol Econ 98: 893-921. [Crossref], [Google Scholar]