

From Quantum Speedup to Practical Advantage

Craig S Wright*

Department of Business, University of Exeter, Exeter, United Kingdom

Corresponding Author: Craig S Wright, Department of Business, University of Exeter, Exeter, United Kingdom, E-mail: craig@rcjbr.org

Received date: 24 September, 2026, **Accepted date:** 08 October, 2026, **Published date:** 14 October, 2026

Citation: Wright CS (2026) From Quantum Speedup to Practical Advantage. *Innov J Appl Sci* 3(5): 55.

Abstract

Quantum computing is often described as evaluating many answers simultaneously. That metaphor confuses a large mathematical state space with accessible classical output and encourages a second mistake: Treating an asymptotic speedup as an engineered or economic result. This commentary revisits Wright against experimental and resource-estimation evidence through 2026 [1]. The central criticism survives, but two claims require revision. Fault tolerance is no longer merely hypothetical after below-threshold logical-memory experiments and cryptanalytic resource estimates have fallen substantially under specified hardware assumptions. The defensible position therefore rests on four distinctions: computability, algorithmic complexity, fault-tolerant execution and practical value. A credible claim of quantum advantage must identify the task, compare against the strongest current classical method, include the complete system cost and explain verification. This framework supports continued research and post-quantum migration while rejecting claims that outrun demonstrated performance.

Keywords: Quantum computing, Quantum advantage, Quantum error correction, Computational complexity, Post-quantum cryptography, Technology assessment

Introduction

The Argument Worth Retaining

An n -qubit pure state is described by 2^n complex amplitudes, but those amplitudes are not an array of independently readable classical answers. A quantum circuit transforms one state. Interference changes the probability distribution over possible measurements and a measurement produces a limited classical outcome. Holevo's theorem constrains the classical information obtainable from ensembles of quantum states, although it should not be treated as a general proof that quantum speedup is impossible [2]. The sharper point is operational: an algorithm must arrange interference so that useful information is recoverable from feasible measurements.

Grover's algorithm illustrates the limit of the popular parallelism metaphor. It offers a quadratic query improvement for unstructured search, not access to every database entry at once [3]. Shor's algorithm obtains period information that supports polynomial-time factoring, but its advantage depends on a structured problem and classical post-processing [4]. These algorithms are genuine. Their success does not convert the exponential dimension of Hilbert space into an exponential volume of output. The core argument of the earlier paper should be stated at that level: state-space size alone is not computational or commercial capacity.

Computability Does Not Decide Efficiency

The Church-Turing thesis concerns which functions are effectively computable. Quantum circuits do not create noncomputable functions, but that fact says little about efficiency. A classical Turing machine can simulate a finite quantum circuit in principle; a direct simulation will generally scale exponentially with qubit number. Complexity theory asks a different question: whether a quantum algorithm solves a specified problem with fewer resources than the best classical algorithm. Conflating these questions makes criticism too easy to dismiss. The absence of hypercomputation does not rule out a separation between bounded-error quantum and classical polynomial time [5].

Experimental advantage is also a moving target. Google's random-circuit experiment showed a large separation from the classical methods used in its original comparison, but later classical techniques reduced that gap [6]. IBM researchers obtained accurate observables from a noisy 127-qubit processor beyond brute-force classical simulation [7]. Tailored tensor-network and sparse-Pauli methods then reproduced those observables more accurately or efficiently [8,9]. This sequence does not make the quantum experiments worthless. It shows why every advantage claim must be dated, task-specific and tested against an improving classical baseline.

Error Correction Changes the Frontier

A blanket claim that scalable fault tolerance is physically impossible no longer fits the evidence. Google Quantum AI and Collaborators demonstrated below-threshold surface-code memories [10]. Their 101-qubit distance-7 code reduced logical error as code distance increased and outlived its best constituent physical qubit. That is the behaviour fault-tolerance theory requires and it is a material experimental achievement.

The result is still a logical memory rather than a general fault-tolerant computer. Useful computation also requires many logical qubits, high-fidelity logical gates, non-Clifford resources, rapid decoding, stable control and successful execution over application-scale circuit depths. Correlated faults, state preparation, measurement and classical control remain part of the machine. The engineering objection should therefore concern measured scaling and complete-system overhead, not an a priori declaration of impossibility. Progress can be real while the distance to economic utility remains large.

Thermodynamic and infrastructure costs remain relevant, but they should be measured rather than asserted to grow exponentially in every architecture. Refrigeration power, control electronics, footprint, fabrication yield and decoder load are engineering quantities whose scaling differs across superconducting, trapped-ion, neutral-atom and photonic systems. A review should therefore avoid transferring a constraint from one platform to the field as a whole. The useful comparison is the marginal resource cost of a verified logical operation at the scale required by a named application.

Cryptographic Risk Requires Current Estimates

Cryptanalytic resource estimates expose another weakness in categorical claims. Gidney and Ekeré estimated that factoring a 2,048-bit RSA modulus in eight hours could require about 20 million noisy qubits under their assumptions [11]. In 2026, Babbush et al. estimated that a `secp256k1` elliptic-curve attack could run in minutes on a fast-clock superconducting architecture using fewer than half a million physical qubits, assuming a physical error rate of 10^{-3} and planar connectivity [12]. These studies address different targets and should not be read as a simple trend line. Their contrast nevertheless shows that resource counts depend strongly on circuit design, architecture, error model and attack objective.

No publicly demonstrated machine can yet execute cryptographic-scale Shor attacks, but migration decisions cannot wait for the final machine. Cryptographic transitions are slow and captured data or exposed public keys may remain valuable. NIST's finalized post-quantum standards therefore support migration as risk management rather than as proof that a cryptographically relevant quantum computer is imminent [13]. A sound threat claim should name the algorithm, key type, exposure window, physical assumptions, runtime and mitigation. Without those quantities, both reassurance and alarm are rhetoric.

A Complete Test for Practical Advantage

Practical advantage requires more than a circuit-level speedup. The claim must first define a useful problem instance, required accuracy and success probability. It must then use the strongest current classical baseline, including specialized algorithms and hardware. The accounting must cover data preparation, compilation, calibration, error correction or mitigation, repeated sampling, decoding, energy and elapsed time. Verification must be possible without assuming the result is correct because classical reproduction is difficult. Finally, the value of the answer must exceed the cost and risk of obtaining it. A quantum processor can win one computational kernel while losing the end-to-end workflow. These tests turn skepticism into a falsifiable research programme rather than a forecast made immune to evidence.

Conclusions

The strongest revision of the original argument is narrower and harder to evade. Quantum computation does not provide freely readable exponential parallelism and no theorem converts algorithmic speedup into practical value. At the same time, error-correction experiments and falling cryptanalytic resource estimates make categorical impossibility claims untenable. The right standard is comparative evidence from complete systems performing useful tasks. That standard leaves room for genuine quantum progress while preventing mathematical possibility, laboratory performance and economic utility from being reported as though they were the same achievement.

Conflict of Interest

The author declares no conflict of interest.

References

1. Wright CS (2025) Quantum computation: An analytical rebuttal. *Journal of Engineering and Artificial Intelligence* 1(1): 17. [Crossref] [GoogleScholar]
2. Holevo AS (1973) Bounds for the quantity of information transmitted by a quantum communication channel. *Problems of Information Transmission* 9(3): 177-183. [GoogleScholar]
3. Grover LK (1997) Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters* 79(2): 325-328. [Crossref] [GoogleScholar]
4. Shor PW (1997) Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing* 26(5): 1484-1509. [Crossref]
5. Bernstein E, Vazirani U (1997) Quantum complexity theory. *SIAM Journal on Computing* 26(5): 1411-1473. [Crossref] [GoogleScholar]
6. Arute F, Arya K, Babbush R, Bacon D, Bardin JC, et al. (2019) Quantum supremacy using a programmable superconducting processor. *Nature* 574: 505-510. [Crossref] [GoogleScholar]

7. Kim Y, Eddins A, Anand S, Wei KX, van den Berg E, et al. (2023) Evidence for the utility of quantum computing before fault tolerance. *Nature* 618: 500-505. [Crossref] [GoogleScholar]
8. Begusic T, Gray J, Chan GKL (2024) Fast and converged classical simulations of evidence for the utility of quantum computing before fault tolerance. *Science Advances* 10(3): eadk4321. [Crossref] [GoogleScholar]
9. Tindall J, Fishman M, Stoudenmire EM, Sels D (2024) Efficient tensor network simulation of IBM's Eagle kicked Ising experiment. *PRX Quantum* 5: 010308. [Crossref] [GoogleScholar]
10. Google Quantum AI and Collaborators (2025) Quantum error correction below the surface code threshold. *Nature* 638: 920-926. [Crossref] [GoogleScholar]
11. Gidney C, Eker M (2021) How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum* 5: 433. [Crossref] [GoogleScholar]
12. Babbush R, Zalcman A, Gidney C, Broughton M, Khattar T, et al. (2026) Securing elliptic curve cryptocurrencies against quantum vulnerabilities: Resource estimates and mitigations. *PRX Quantum* 7: 031001. [Crossref] [GoogleScholar]
13. National Institute of Standards and Technology (2024) Post-quantum cryptography.

Copyright: © 2026 The Author(s). Published by Innovative Journal of Applied Science. This is an open-access article under the terms of the Creative Commons Attribution License (CC BY). (<https://creativecommons.org/licenses/by/4.0/>).