Potomac Institute for Policy Studies presents

TECH HAPPENS

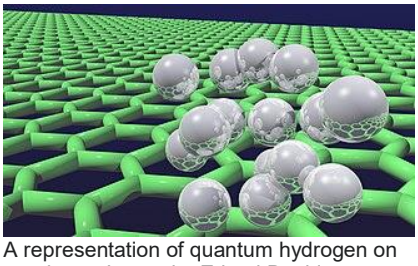
Tech Happens© *provides short articles on critical technology and policy issues, their effects on our lives today, and impact to the future.*

Are Quantum Computers the Next Big Thing?

September 2, 2025

Since the 1980s, researchers around the world have been working on developing a "quantum computer." Based on theories of quantum physics and work of Feynman and Benioff, the theoretical concept has matured to the point of some operational machines. But there are issues.

The draw is the hope that NP problems, and in especially NP-hard problems can succumb to a quantum computer. NP problems generally require a non-deterministic machine to solve the problem in a reasonable (polynomial in the size of the input) amount of time. But, alas, a quantum computer is not a non-deterministic machine. However, using probabilistic algorithms, there are still difficult problems that can be solved with a quantum computer that cannot be solved in reasonable time with a classical computer.



A representation of quantum hydrogen on graphene. Image by Erlend Davidson (Thomas Young Centre, London)

One such problem is the problem of prime factorization. Shor's Algorithm for a quantum computer can theoretically break the gold standard for encryption, the RSA algorithm. But quantum computers are many orders of magnitude short in terms of number of qubits and time of coherence before Shor's Algorithm can be applied to practical encryption keys. So, when we hear of improvements in number of qubits (and improvements in coherence times), rest assured that we are still a long way off

from the encryption nightmare (maybe 10 orders of magnitude for each of number of qubits and coherence time).

On the other hand, quantum computers are potentially valuable because of two other algorithmic methods. Grover's quantum computer algorithm provides a probabilistic method to do database searches that provides (quadratic) speedup over sequential search and might be useful for certain optimization algorithms.

But the real benefit of a quantum computer might be in applications for quantum annealing, to provide a more general optimization algorithm, useful in many applications including LLM training for AI applications.

Quantum computers for quantum annealing have a bad rap, because early D-Wave machines were found to not provide significant speed-up over simulated annealing, which could be done on classical computers. But with a very few orders of magnitude increases in number of qbits and coherence times, large speedups are theoretically possible. Annealing uses quantum entanglement and thus coherence to allow "tunneling" to avoid false minima but extending memory times of quantum states could perhaps accomplish the same thing. An order of magnitude improvement (or more) in memory for quantum computers has been discovered using phonons, i.e., sound waves.

Will this allow quantum annealing to achieve speedup in practical applications? Maybe. As tech happens, applications are found.