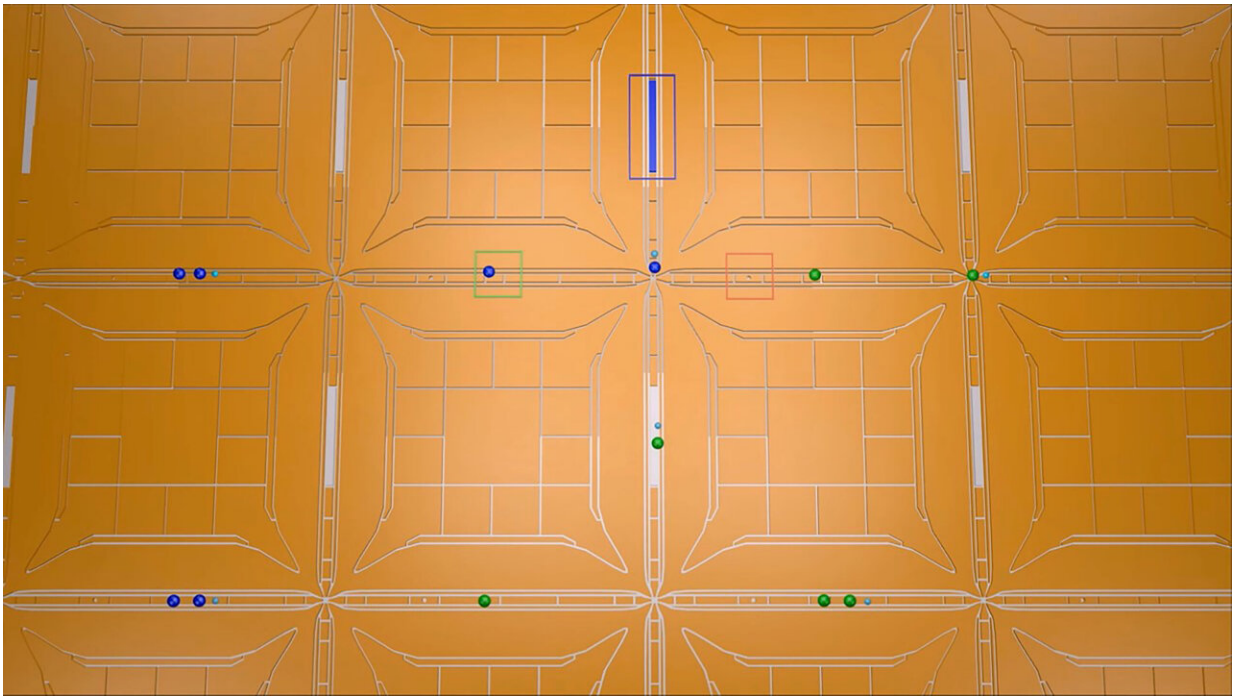
How big does your quantum computer need to be?

January 25 2022



Quantum computer blueprint with trapped ions. Credit: Ion Quantum Technology Group, University of Sussex

Quantum computers are expected to be disruptive and potentially impact many industry sectors. So researchers in the United Kingdom and the Netherlands decided to explore two very different quantum problems: breaking the encryption of Bitcoin (a digital currency) and simulating the molecule responsible for biological nitrogen fixation.

In *AVS Quantum Science*, the researchers describe a tool they created to determine how big a quantum computer needs to be to solve problems like these and how long it will take.

"The majority of existing work within this realm focuses on a particular hardware platform, superconducting devices, like those IBM and Google are working toward," said Mark Webber, of the University of Sussex. "Different hardware platforms will vary greatly on key hardware specifications, such as the rate of operations and the quality of control on the qubits (quantum bits)."

Many of the most promising quantum advantage use cases will require an error-corrected quantum computer. Error correction enables running longer algorithms by compensating for inherent errors inside the quantum computer, but it comes at the cost of more physical qubits.

Pulling nitrogen out of the air to make ammonia for fertilizers is extremely energy-intensive, and improvements to the process could impact both world food scarcity and the climate crisis. Simulation of relevant molecules is currently beyond the abilities of even the world's fastest supercomputers but should be within the reach of next-gen quantum computers.

"Our tool automates the calculation of the error-correction overhead as a function of key hardware specifications," Webber said. "To make the quantum algorithm run faster, we can perform more operations in parallel by adding more physical qubits. We introduce extra qubits as needed to reach the desired runtime, which is critically dependent on the rate of operations at the physical hardware level."

Most quantum computing hardware platforms are limited, because only qubits right next to each other can interact directly. In other platforms, such as some trapped ion designs, the qubits are not in fixed positions

and can instead be physically moved around—meaning each qubit can interact directly with a wide set of other qubits.

"We explored how to best take advantage of this ability to connect distant qubits, with the aim of solving problems in less time with fewer qubits," said Webber. "We must continue to tailor the error-correction strategies to exploit the strengths of the underlying hardware, which may allow us to solve highly impactful problems with a smaller-size quantum computer than had previously been assumed."

Quantum computers are exponentially more powerful at breaking many encryption techniques than classical computers. The world uses RSA encryption for most of its secure communication. RSA encryption and the one Bitcoin uses (elliptic curve digital signature algorithm) will one day be vulnerable to a quantum computing attack, but today, even the largest supercomputer could never pose a serious threat.

The researchers estimated the size a quantum computer needs to be to break the encryption of the Bitcoin network within the small window of time it would actually pose a threat to do so—in between its announcement and integration into the blockchain. The greater the fee paid on the transaction, the shorter this window will be, but it likely ranges from minutes to hours.

"State-of-the-art quantum computers today only have 50-100 qubits," said Webber. "Our estimated requirement of 30 [million] to 300 million physical qubits suggests Bitcoin should be considered safe from a quantum attack for now, but devices of this size are generally considered achievable, and future advancements may bring the requirements down further.

"The Bitcoin network could perform a 'hard-fork' onto a quantum-secure encryption technique, but this may result in network scaling issues due to

an increased memory requirement."

The researchers emphasize the rate of improvement of both quantum algorithms and error- correction protocols.

"Four years ago, we estimated a trapped ion device would need a billion physical qubits to break RSA encryption, requiring a device with an area of 100-by-100 square meters," said Webber. "Now, with improvements across the board, this could see a dramatic reduction to an area of just 2.5-by-2.5 square meters."

A large-scale error-corrected quantum computer should be able to solve important problems classical computers cannot.

"Simulating molecules has applications for energy efficiency, batteries, improved catalysts, new materials, and the development of new medicines," said Webber. "Further applications exist across the board—including for finance, big data analysis, fluid flow for airplane designs, and logistical optimizations."

More information: "The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime" *AVS Quantum Science*, DOI: 10.1116/5.0073075

Provided by American Institute of Physics