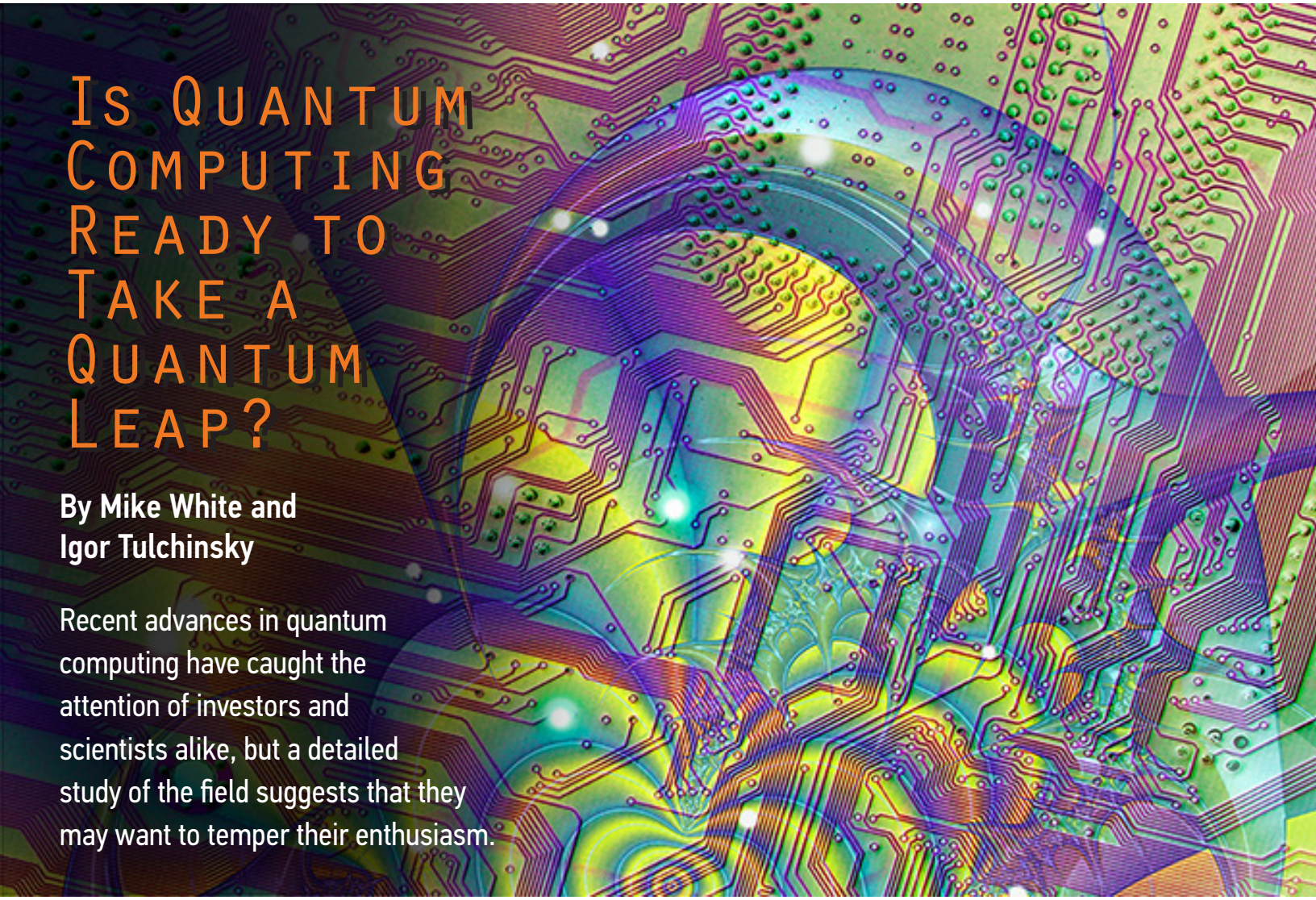
04.24.17

WorldQuant Perspectives



Is Quantum Computing Ready to Take a Quantum Leap?

By Mike White and Igor Tulchinsky

Recent advances in quantum computing have caught the attention of investors and scientists alike, but a detailed study of the field suggests that they may want to temper their enthusiasm.

WORLDQUANT®

WorldQuant, LLC
1700 East Putnam Ave.
Third Floor
Old Greenwich, CT 06870
www.weareworldquant.com

COULD 2017 BE THE YEAR THAT QUANTUM COMPUTING MOVES into the mainstream? A recent article in the journal *Nature* makes such a claim. In February an international team of researchers, led by the Ion Quantum Technology Group at Sussex University in the U.K., published what it describes as an industrial blueprint on how to build a large-scale quantum computer. The Sussex team, headed by physicist Winfried Hensinger, is using the plan to construct a prototype device, which it expects to complete within two years. Hensinger estimates that a full-scale ion-trap quantum computer built to the team's specifications would fill a building larger than a football field, require ten years of development and cost up to £100 million ($126 million).

The Sussex-led project is just the latest news in the oft-hyped field of quantum computing. Tech giants Google, IBM and Microsoft have all announced significant progress in their research efforts; quantum computing start-ups continue to decloak from stealth mode; and academic labs have been announcing major breakthroughs. Physicist Leo Kouwenhoven of Station Q — Microsoft's worldwide research consortium on quantum computing, founded on the campus of the University of California, Santa Barbara — said recently in an interview, "I tell my students that 2017 is the year of braiding." The braiding Kouwenhoven is referring to is a key component of Microsoft's quantum computing effort, which to date has never been realized.

D-Wave Systems, a Canadian company that claims to have shipped the first-ever commercially available quantum computer, in 2012, released the latest version of its system in January. Google, Lockheed Martin and NASA are all D-Wave customers. Cybersecurity company Temporal Defense Systems is the first customer for the $15 million D-Wave 2000Q quantum computer.

> "David Deutsch was the first to explicitly suggest exploiting quantum superposition and entanglement, igniting the race to build a working quantum computer."

Nobel Origins

In 1981, Nobel Prize–winning physicist Richard Feynman gave a talk at the First Conference on the Physics of Computation, during which he observed that it appeared to be impossible, in general, to simulate the evolution of a quantum system on a classical computer in an efficient way. However, he also proposed a basic model for a quantum computer that would be capable of such simulations. A year later Paul Benioff, working at the Department of Energy's Argonne National Laboratory, suggested a computer model based on the Turing machine but using quantum dynamics. In 1985, David Deutsch of Oxford University formulated a type of quantum Turing machine and an algorithm to run on it. In doing so, Deutsch was the first to explicitly suggest exploiting quantum superposition and entanglement, igniting the race to build a working quantum computer.

Classical computers store information as bits, which represent either a 1 or a 0. Quantum bits — also known as qubits — rely on the quantum effect of superposition, which allows a qubit to take on the 0 and 1 states at the same time. A string of ten qubits can, therefore, represent all 1,024 ten-bit numbers simultaneously. Many quantum computer designs utilize another quantum effect: entanglement. Quantum entanglement enables a qubit to share its state with other qubits, inextricably linking them no matter the distance among entangled qubits. Quantum superpositions and entanglements are, however, extremely fragile and can be destroyed by perturbations from the environment or even from the simple act of measuring the state of a qubit, an effect known as decoherence. Much of the effort that has been expended in the field of quantum computing has gone toward stabilizing these effects and developing error correction schemes.

Array of Approaches

Scientists have adopted an array of approaches to the challenge of creating stable qubits and, ultimately, a working quantum computer. Using the stable electronic states of trapped ions (charged atoms) to store qubits is a method that has been studied for decades and is the basis for College Park, Maryland–based start-up IonQ's technology. In this approach's most common configuration, tuned lasers cool and trap the ions and place them in superposition states. This approach produces relatively stable qubits, but the many lasers required create complexity and impose challenges on scalability. As of May 2011 the largest number of entangled qubits was 14.

Superconducting loops — favored by Google and New Haven, Connecticut–based start-up Quantum Circuits — utilize a resistance-free circuit in which an electrical current oscillates. An injected microwave signal excites the current into superposition states. Superconducting loops have to be cooled to extremely low temperatures to operate and are quite unstable, which causes the qubits to be not long-lived. Google has so far produced a nine-qubit computer and plans to achieve "quantum supremacy" by outperforming the world's top supercomputers on a particular memory-intensive task with a 50-qubit quantum computer. The memory required for the task is on the order of 2.25 petabytes (roughly 2.4 million gigabytes) — almost double that of the top public supercomputer in the world. Scientists familiar with Google's progress claim that the company could achieve its goal by the end of this year.

In contrast, Microsoft has been working for more than a decade on topological quantum computers. This approach utilizes quasiparticles called anyons and encodes information (qubits) in the order in which the anyons swap position, an effect known as braiding. (Imagine the anyons dragging a thread behind them. As they orbit one another, they braid that thread into a pattern, which encodes the logic gates of the computer.) Because topological quantum computers don't rely on the state of individual particles in superposition, they can operate at a higher level of precision and thus require less error correction.

Controversial Claims

D-Wave is betting on adiabatic quantum computing. The D-Wave system implements a quantum annealing algorithm and is not a general-purpose quantum computer — it requires a developer to formulate a problem in a particular manner. Quantum annealing can be thought of in terms of the analogy of a mountain range where the altitude of the landscape represents the energy (or cost) of a solution. The aim is to find the lowest point on the mountain range and read off the coordinates. Classical approaches are akin to traipsing around the mountains to find the lowest point. Quantum annealing makes use of yet another spooky quantum effect — tunneling — to pass through hills, reducing the chance of being trapped in valleys that are not the global minimum. The quantum entanglement among the qubits is said to improve the outcome by revealing correlations in the coordinates that lead to deep valleys. D-Wave remains somewhat controversial among quantum physicists, with claims and counterclaims as to whether its devices are actually quantum in nature.

> "D-Wave remains somewhat controversial among quantum physicists, with claims and counterclaims as to whether its devices are actually quantum in nature."

In May 2016, IBM made its five-qubit quantum computer publicly accessible via its cloud platform. Superficially similar to the D-Wave system in that they both utilize superconducting quantum interference devices (SQUIDs) — very sensitive magnetometers that are used to measure extremely subtle magnetic fields — the IBM machine is billed as a universal quantum computer. Rather than emphasizing computation (which with just five qubits is significantly limited), IBM has focused on demonstrating that its device computes reliably through its strong error correction. Producing a quantum computer that is reliable enough to be online 24-7 is another significant milestone. IBM plans to be able to scale to between 50 and 100 qubits within the next decade.

Diamond-Based Solution

Research at the Massachusetts Institute of Technology is being carried out on the use of nitrogen-vacancy (NV) centers in synthetic diamonds to create qubits. A pure diamond consists of carbon atoms arranged in a regular lattice structure. Missing carbon nuclei constitute vacancies in the lattice. If a nitrogen atom takes the place of a carbon atom adjacent to the vacancy, a nitrogen vacancy is created. A powerful magnetic field can influence the spin of the NV center, creating qubits in superposition. One strength of this method is that the diamond lattice forms a natural confinement system for the qubit, dispensing with the complex hardware that is used to trap ions or that other approaches require. Somerville, Massachusetts, start-up Quantum Diamond Technologies is hoping to commercially exploit NV-diamond technology, particularly within the biomedical and diagnostic fields.

Among semiconductor companies, Intel Corp. is working with researchers in the Netherlands at TU Delft's QuTech quantum research institute on a chip they hope will facilitate quantum computing. In their design the spin of a single electron is trapped inside a modified transistor. The chip leverages conventional silicon transistor fabrication technologies, which may allow for scaling to hundreds of thousands of qubits on a single wafer.

The Sussex team's ion-trap quantum computer design tackles many of the practical issues that have beset the construction of large-scale quantum computers. Rather than use individual lasers to control each trapped ion — which would be hugely complex at scale — the design employs a handful of global microwave fields in conjunction with powerful magnetic gradients applied locally to each gate. The team tackles the complexity of building a quantum computer containing millions or even billions of qubits through a modular design that makes use of the silicon fabrication techniques already employed in the electronics industry. Each module contains a 36-by-36 array of X-junction ion traps designed so that ions can be directly shuttled from one module to another instead of using optical interconnects, as previous work has proposed. Modules are aggregated into octagon-shaped ultra–high vacuum chambers, with a single chamber 4.5 square meters in size containing more than 2.2 million individual ion traps.

No Silver Bullet

But what exactly could be possible with a working quantum computer? Quantum computation is not a silver bullet: Quantum machines cannot compute all nondeterministic polynomial (NP) problems in polynomial time. Quantum computers require quantum algorithms, and not all quantum algorithms produce exponential speedup. Quantum algorithms are probabilistic in nature, giving the correct answer with high probability — the probability of failure can be decreased by repeating the algorithm. Quantum algorithms are often described by a quantum circuit, which acts on some number of input qubits and terminates with a measurement (the result). The quantum circuit consists of basic building blocks called quantum gates, which operate on a fixed number of qubits (usually two or three).

Two of the better-known quantum algorithms are Shor's algorithm and Grover's algorithm. In 1994, Peter Shor, working at AT&T's Bell Laboratories, formulated an algorithm that would enable a quantum computer to factor large integers quickly. RSA cryptosystems, which are widely used for securing data transmission and transactions on the Internet, rely on the fact that factoring large numbers is difficult. The popular belief is that a working implementation of Shor's algorithm would mean the end of Internet privacy. The truth, though, is likely somewhat less apocalyptic, as scientists and government agencies are already working on postquantum cryptography. The Sussex team estimates that a Shor factorization of a 2,048-bit number would take on the order of 110 days and require 2 billion trapped ions in its formulation of a quantum computer. A tenfold reduction in the error probability, however, would allow the quantum computer to factorize the 2,048-bit number in about ten days, using 500 million trapped ions.

Devised by Lov Grover in 1996, Grover's algorithm is often described as a database search algorithm that looks for a specified entry in an unordered database. Grover's algorithm employs an important technique in quantum algorithm design, known as amplitude amplification, to achieve a polynomial speedup over the best classical algorithms. Grover's algorithm can be used for estimating the mean and median of a set of numbers and has application in speeding up any problem previously solved using brute-force methods.

Progress Being Made

Despite the hype, finding concrete examples of applications of quantum computing to finance is surprisingly difficult. For many years journalists and bloggers have been pointing in the general direction of portfolio optimization, financial risk calculation and machine learning, but there are few bodies of research that describe in detail how these might be implemented on a quantum computer, even from a theoretical perspective. Recently, though, there are hints that financial institutions are starting to take notice of the progress being made in the field of quantum computing — and it may not just be due to the obvious investment potential that the start-ups in the area represent. Goldman Sachs is an investor in D-Wave Systems, and Bloomberg reports, rather vaguely, that it is "considering using the technology." Both CME

> "Quantum computers require quantum algorithms, and not all quantum algorithms produce exponential speedup."

Ventures and RBS Silicon Valley Solutions have invested in 1QBit, a Vancouver-based company that creates optimization software for D-Wave machines. This month the Commonwealth Bank of Australia purchased a Quantum Computing Simulator System from QXBranch with the goal of assessing "the feasibility and performance of applications well before the first silicon quantum computer is finished." QXBranch, a Washington, DC–headquartered quantum computing and data analytics firm, previously hosted a first-of-a-kind, all-day hackathon where algo traders competed to solve problems using quantum computing techniques

In 2016, D-Wave Systems and 1QBit partnered with financial industry representatives to launch the Quantum for Quants online community, with a mission to foster "education, discussion, and industry collaboration on open industry problems." Marcos López de Prado, a senior managing director at investment firm Guggenheim Partners and managing editor of Quantum for Quants, lists the following immediate practical applications of quantum computing in finance: generalized multihorizon portfolio optimization, clustering, scenario simulations and options pricing. Research made available on 1QBit's website documents formulations for finding optimal arbitrage opportunities using quantum annealing and a quantum-ready approach to portfolio optimization.

A second paper on multiperiod portfolio optimization describes an actual implementation of the approach on both 512-qubit and 1,152-qubit D-Wave systems. A necessary component of the experimentation was to map the problem graph to the physical topology of the D-Wave hardware: Within the D-Wave computers, qubits are not connected together globally, but eight-qubit cells are sparsely coupled into a topology known as a Chimera graph. To account for this, multiple physical qubits must be coupled together into logical qubits, a procedure called "minor embedding." Results are published for multiperiod portfolio optimizations with a maximum complexity of a portfolio comprising six assets modeled over six time steps.

Applications For Machine Learning

Although not directly a financial application, quantum machine learning is currently an area of intense research. In this discipline quantum machine learning algorithms utilize the capabilities offered by quantum computation to enhance classical methods of machine learning.

Some have claimed that quantum machine learning can provide exponential speedup over classical algorithms. Quantum machine learning algorithms encode a classical data set into a quantum computer, turning it into quantum information. Quantum information-processing routines are applied, and the result of the computation is then read out through measurement of the quantum system. The outcome of the measurement of a qubit might indicate the result of a binary classification task, for example.

Quantum matrix inversion — based on the HHL algorithm for linear systems of equations — can be applied to machine learning techniques where the training reduces to solving a linear system of equations (for example, least squares linear regression). Many quantum machine learning algorithms use techniques based on Grover's search algorithm, accelerating learning algorithms that translate into unstructured search tasks. Quantum computing–

> "Some have claimed that quantum machine learning can provide exponential speedup over classical algorithms."

enhanced unsupervised learning methods use this approach: K-medians, hierarchical clustering and quantum manifold embedding. Quantum annealing is also being explored in the training of Boltzmann machines and deep neural networks.

It seems highly improbable that a general-purpose quantum computer will be available for purchase this year. Still, it does seem possible that someone with extremely deep pockets could start to construct one in the next several years. (Within trapped-ion quantum computing, for example, most of the seemingly intractable problems look to have answers, albeit expensive ones.) If that happens, machine learning could get a boost as some firms turn to quantum computing to accelerate their existing efforts.

Mike White is Director of Software Infrastructure at WorldQuant, LLC and has a Ph.D. in evolutionary computing from the University of London. Igor Tulchinsky is founder, chairman and CEO of WorldQuant, LLC.

Thought Leadership articles are prepared by and are the property of WorldQuant, LLC, and are circulated for informational and educational purposes only. This article is not intended to relate specifically to any investment strategy or product that WorldQuant offers, nor does this article constitute investment advice or convey an offer to sell, or the solicitation of an offer to buy, any securities or other financial products. In addition, the above information is not intended to provide, and should not be relied upon for, investment, accounting, legal or tax advice. Past performance should not be considered indicative of future performance. WorldQuant makes no representations, express or implied, regarding the accuracy or adequacy of this information, and you accept all risks in relying on the above information for any purposes whatsoever. The views expressed herein are solely those of WorldQuant as of the date of this article and are subject to change without notice. No assurances can be given that any aims, assumptions, expectations and/or goals described in this article will be realized or that the activities described in the article did or will continue at all or in the same manner as they were conducted during the period covered by this article. WorldQuant does not undertake to advise you of any changes in the views expressed herein. WorldQuant may have a significant financial interest in one or more of any positions and/or securities or derivatives discussed.