MIT
Technology
Review

Entangled Light, Quantum Money

A breakthrough explores the challenges–and suggests the financial possibilities–of creating quantum networks.

By Mark Williams Pontin

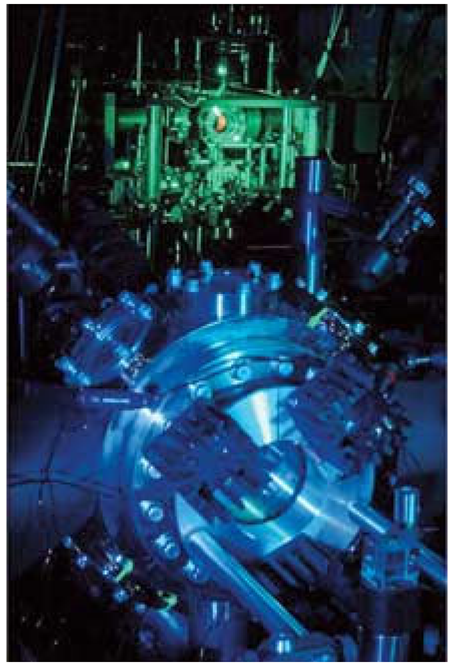
August 18, 2009

In recent years, the Austrian physicist Anton Zeilinger has bounced entangled photons off orbiting satellites and made 60-atom fullerene molecules exist in quantum superposition–essentially, as a smear of all their possible positions and energy states across local space-time. Now he hopes to try the same stunt with bacteria hundreds of times larger. Meanwhile, Hans Mooij of the Delft University of Technology, with Seth Lloyd, who directs MIT’s Center for Extreme Quantum Information Theory, has created quantum states (which occur when particles or systems of particles are superpositioned) on scales far above the quantum level by constructing a superconducting loop, visible to the human eye, that carries a supercurrent whose electrons run simultaneously clockwise and counterclockwise, thereby serving as a quantum computing circuit.

POPULAR

The 8 worst technology failures of 2024
Antonio Regalado

AI can now create a replica of your personality
James O'Donnell



Two Nodes of a quantum network that Caltech researchers created by halting entangled photons within two ensembles of cesium atoms housed in an ultrahigh-vacuum system. Temporarily storing entanglement provides a basis for quantum data storage, which might be useful for various applications, including quantum cryptography.

The physicist Richard Feynman proposed the idea of quantum computing in 1981 to exploit the information-processing potential of atoms, photons, and elementary particles. By now, the field has advanced sufficiently far that researchers not only are able to manipulate physics for unprecedented experimental effects but have proposed commercial applications.

But before technologies like quantum communications, computing, and metrology can realize their potential–a quantum Internet and uncounterfeitable money are two interesting possibilities–quantum networks must be able to transmit and store data. The quantum optics group at the California Institute of Technology has been working toward this goal. The team is headed by H. Jeff Kimble, Valentine Professor of Physics, who led the 1998 effort that achieved the first unambiguous teleportation of one photon's quantum state–that is, the information represented by its spin, energy, and such–to another photon. Now Kimble and his team have demonstrated a way for entanglement–the nonlocal relationship that allows quantum teleportation, which Einstein skeptically dismissed as "spooky action at a distance"–to be created in networks.

Much as the motion of electrons in microprocessor circuits transmits data within today's computers, the teleportation of quantum states between entangled particles would perform that task in quantum networks. As for data storage, says Kyung Soo Choi, a researcher in Kimble's group, a central question that one of their recent experiments resolved was, "How do you convert entangled light into an entanglement of matter and back into light?" Entangled states are fragile, and networks of entangled light will require repeating devices–much the way long-distance fiber-optic networks require optoelectronic repeating devices to regenerate diminishing signals. Therefore, entanglement will need to be generated and stored in component subsystems within a greater quantum network. Now Kimble and his team have demonstrated a technical solution to the problem.

RESOURCES:
"Functional Quantum Nodes for Entanglement Distribution over Scalable Quantum Networks"
Chin-Wen Chou, Julien Laurat, Hui Deng, Kyung Soo Choi, Hugues de Riedmatten, Daniel Felinto, and H. Jeff Kimble
Science 316: 1316–1320 (2007)

"Mapping Photonic Entanglement into and out of a Quantum Memory"
K. S. Choi, H. Deng, J. Laurat, and H. J. Kimble
Nature 452: 67–71 (2008).

The Caltech team used two ensembles of cesium atoms whose states they influenced with a laser, making them either transparent or opaque as needed to manipulate incoming photons' speeds. The researchers then split single photons, putting them in superposition–that is, they were part of the same quantum wave function and, thus, entangled–while ensuring that they propagated along two paths into the two cesium ensembles. Choi explains, "We slowed the light to a crawl and halted it inside the matter by deactivating the control laser that was making the cesium ensembles transparent, so the quantum information–the entangled light–was stored inside the atomic ensembles. By reactivating the control laser, we reaccelerated the photons to normal speed, restoring the beams of entangled light." So far, the Caltech researchers have stored entanglement in matter for spans of one microsecond. Kimble estimates that he and his team can extend that to 10 microseconds.

Kimble possesses a courtly Texas gentleman's manner, as I discovered after his lab manager found him 15 minutes on the schedule following two weeks when the physicist was away, making presentations at four conferences on two continents. Those 15 minutes became a tutorial on recent technical advances in verifying and quantifying entanglement. Measurement is the central problem in quantum mechanics, since any particle or system exists in a quantum state only until another system, whether one as slight as a stray air molecule or as complex as a human observer, gains information about it and thereby collapses that state. This is mind-bendingly abstruse stuff. Aside from discussing quantum metrology, though, Kimble made one easily graspable assertion: "Our society's technical base is information commerce. In the next 20 years, quantum information science–a fusion of computer science and quantum mechanics that didn't exist 20 years ago–will radically change that commerce."

The revolutionary technology that Kimble envisions is large quantum networks, resembling the Internet but relying on entanglement. What inherent advantages would promote the development and adoption of such networks?

Substantial ones. Quantum networks have already been built on a limited scale. In 2004, the world's first permanent quantum cryptography system was activated in Cambridge, MA, linking Harvard, Boston University, and DARPA contractor BBN Technologies (formerly known as Bolt Beranek and Newman, under which name the company created the original ARPAnet). Today, id Quantique, a Swiss company, and MagiQ Technologies, a U.S. one, offer commercial modules using optical fiber to transmit quantum keys, in the form of photons encoded as bits by controlling their polarization, over limited distances that top out at about 100 kilometers. Since attempted interception of these light particles would disturb their state and expose eavesdropping, such quantum cryptography systems offer absolute data security.

Furthermore, the prospect of quantum computing was what provided the initial impetus for research into quantum networks. If such computing can be done seriously (so far, experiments have used at most seven qubits, or quantum binary digits), it promises to surpass classical computing in significant respects. Scott Aaronson, an MIT expert on computational complexity, cites the algorithm published in 1994 by MIT mathematician Peter Shor as the breakthrough that proved quantum computing a viable proposition by demonstrating that it could factor very large numbers in reasonable computing time. Because that task has been beyond classical computers, most public-key cryptography has hitherto been based on factoring large numbers. But it would be vulnerable to cryptanalysis based on quantum computing. As Aaronson says, "That's why the National Security Agency is interested in quantum computing." Quantum cryptography, however, would offer data security against quantum code-breaking as well as against regular cryptanalysis.

Besides ensuring the security of data, the quantum wide-area repeater networks, or QWANs, that Kimble has in mind would possess few of current networks' latency issues–indeed, could be as nearly instantaneous as light speed allows. Moreover, the exponential parallelism that would give quantum computing its power–with two entangled particles, or qubits, representing four different values, four qubits 16 values, and so on–ought to apply to networks of quantum computing devices. Kimble says, "Though there'll be a largest size attainable for the state space of individual quantum processing units, it'll be possible to surpass that by linking those units together into a fully quantum network." A quantum computer's "state space" is the full range of potential states in which the computer could exist. When a quantum algorithm is run, this computational process collapses that state space and shrinks the computer's range of possible states down to a single one: the correct answer to the given problem. With a network of quantum computers, Kimble is claiming, the exponential computational power of each device would be multiplied exponentially.

MIT’s Seth Lloyd has given some thought to the design options for quantum networks. He says, “Networks using cesium-atom ensembles are one of the most promising technologies for transporting quantum information over long distances.” Yet the ensemble approach is relatively bulky, and the larger a quantum system, the greater the problems for computing. Lloyd says, “Circuit-based approaches like superconducting loops are more scalable within a small space, with potentially large numbers of qubits on one circuit board.” But such systems are unsuitable for communications. “Kimble and I have collaborated on concepts using individual atoms instead of ensembles,” he says. “If we could move information between atomic ensembles and individual ions and ion traps, that’s a scalable quantum technology.” A plausible scenario, according to Lloyd, seems to be to use ensembles for communications and the more localized, scalable quantum devices, like the superconducting loops or the ion traps, for computation.

So Kimble has a reasonable argument that quantum networks are feasible. And the advantages that he envisions–absolute data security, no latency, and a further exponential gain in computational power–would hardly be negligible in the world of information commerce.

Some commercial applications of quantum information technology are fairly obvious. Human stock traders have come to rely on the computerized trading programs known as high-frequency traders (HFTs). On some days, these generate more than half the volume on the New York Stock Exchange. Major trading institutions have spent millions developing their algorithms to analyze market data and execute large numbers of trades according to strategies that are, mostly, sophisticated variations on buying microseconds after some data arrives and then selling microseconds later at the expense of other traders who couldn’t get the data in or their trades out as rapidly. Futures traders who use near-instantaneous quantum networks will have clear advantages over those who don’t.

Other commercial applications are possible as well. Scott Aaronson suggested one of them in a paper called “Quantum Copy-Protection and Quantum Money.” He observed that quantum states cannot be copied because any measurement process destroys them, which “raises the possibility of using quantum states as unclonable information.” Exploiting this possibility will require circumventing the fact that quantum states collapse under measurement and creating, first (for purposes of quantum money), unclonable states that can be verified as authentic, and second (for purposes of quantum copy protection), unclonable states that would still allow the protected software, DVDs, CDs, and so on to be used. Aaronson demonstrated that at least one type of publicly verifiable quantum money and two schemes for quantum-based copy protection are theoretically feasible–raising the possibility, for the first time ever, of absolutely uncounterfeitable money and insurmountable digital-rights protection.

The first generation of money emerged with the invention of coins in Lydia nearly 3,000 years ago, its second generation with the paper bills of exchange issued by the banks of Renaissance Italy, and its third with electronic money and the virtual economy of the modern era. If scientists like Kimble and Aaronson are correct, quantum networks may soon give rise to a further generation of money.

Mark Williams is a contributing editor to *Technology Review.*

by Mark Williams Pontin