Quantum Computing: A New Beginning

Ramsés Gallego
CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT, Six Sigma Black Belt
Chief Technologist Cybersecurity, DXC Technology
ISACA Hall of Fame

Past International Vice President, ISACA, Board of Directors
President, ISACA Barcelona Chapter
Executive Vice President, Quantum World Association
Privacy by Design Ambassador, Government of Ontario, Canada
ramses.gallego@me.com @rams𝕏gallego

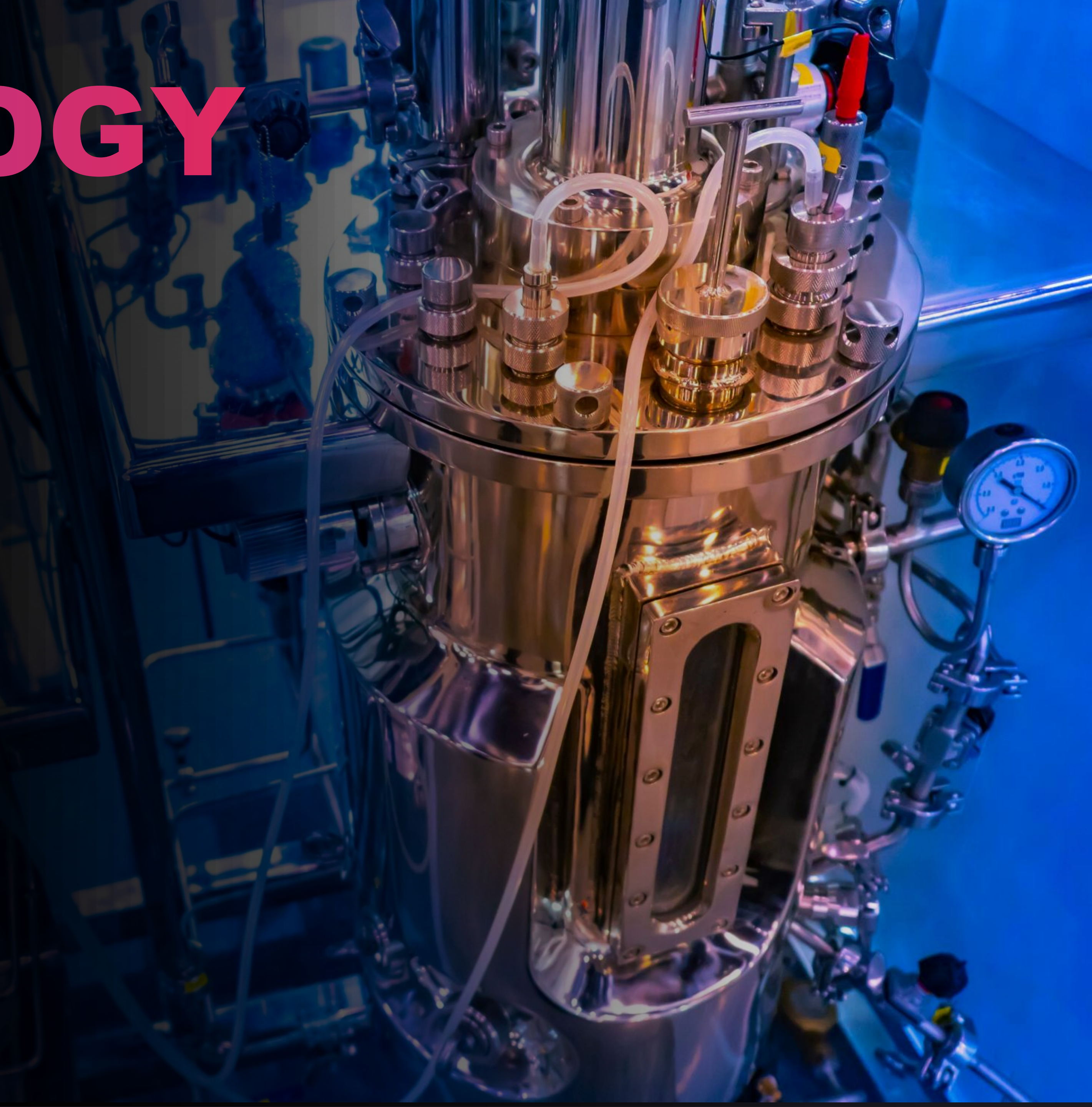
DXC TECHNOLOGY

ISACA®

the
future
is
now

Quantum computing

TERMINOLOGY



Qubits

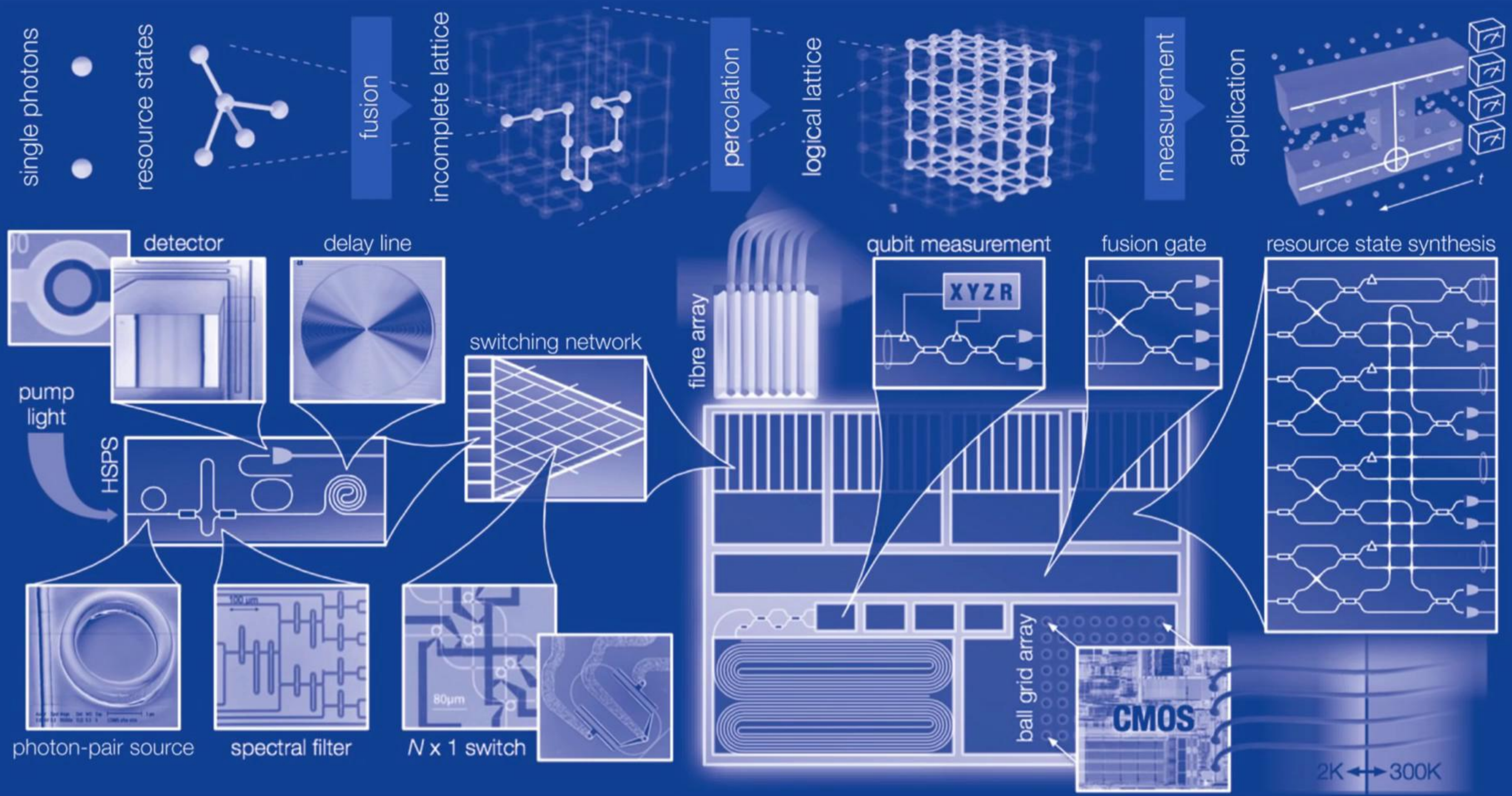
Superposition

Entanglement

Photons

Encryption

BLUEPRINT FOR A QUANTUM COMPUTER



The three known types of quantum computing and their applications, generality, and computational power.

A very specialized form of quantum computing with unproven advantages over other specialized forms of conventional computing.

DIFFICULTY LEVEL

●●○○○○○○○○

Quantum Annealer

The quantum annealer is least powerful and most restrictive form of quantum computers. It is the easiest to build, yet can only perform one specific function. The consensus of the scientific community is that a quantum annealer has no known advantages over conventional computing.

APPLICATION
Optimization Problems

GENERALITY
Restrictive

COMPUTATIONAL POWER
Same as traditional computers

The most likely form of quantum computing that will first show true quantum speedup over conventional computing. This could happen within the next five years.

DIFFICULTY LEVEL

●●●●○○○○○○

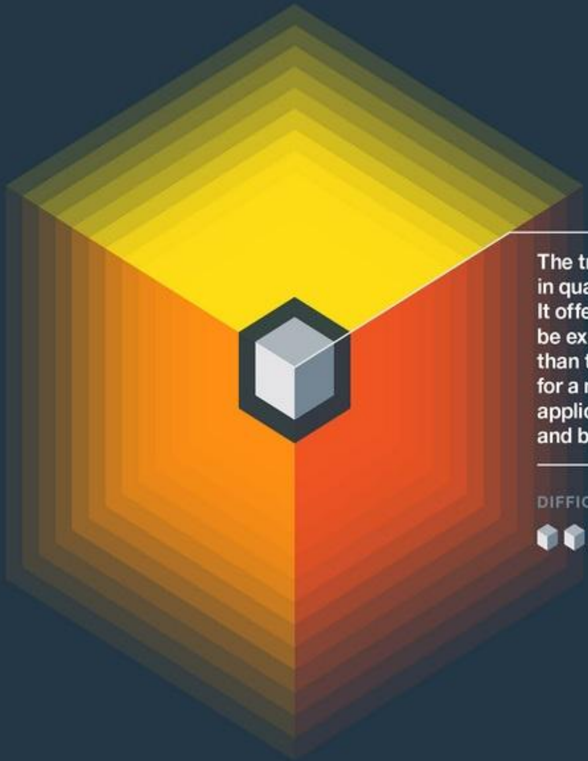
Analog Quantum

The analog quantum computer will be able to simulate complex quantum interactions that are intractable for any known conventional machine, or combinations of these machines. It is conjectured that the analog quantum computer will contain somewhere between 50 to 100 qubits.

APPLICATIONS
Quantum Chemistry
Material Science
Optimization Problems
Sampling
Quantum Dynamics

GENERALITY
Partial

COMPUTATIONAL POWER
High



The true grand challenge in quantum computing. It offers the potential to be exponentially faster than traditional computers for a number of important applications for science and businesses.

DIFFICULTY LEVEL

●●●●●●●●●●

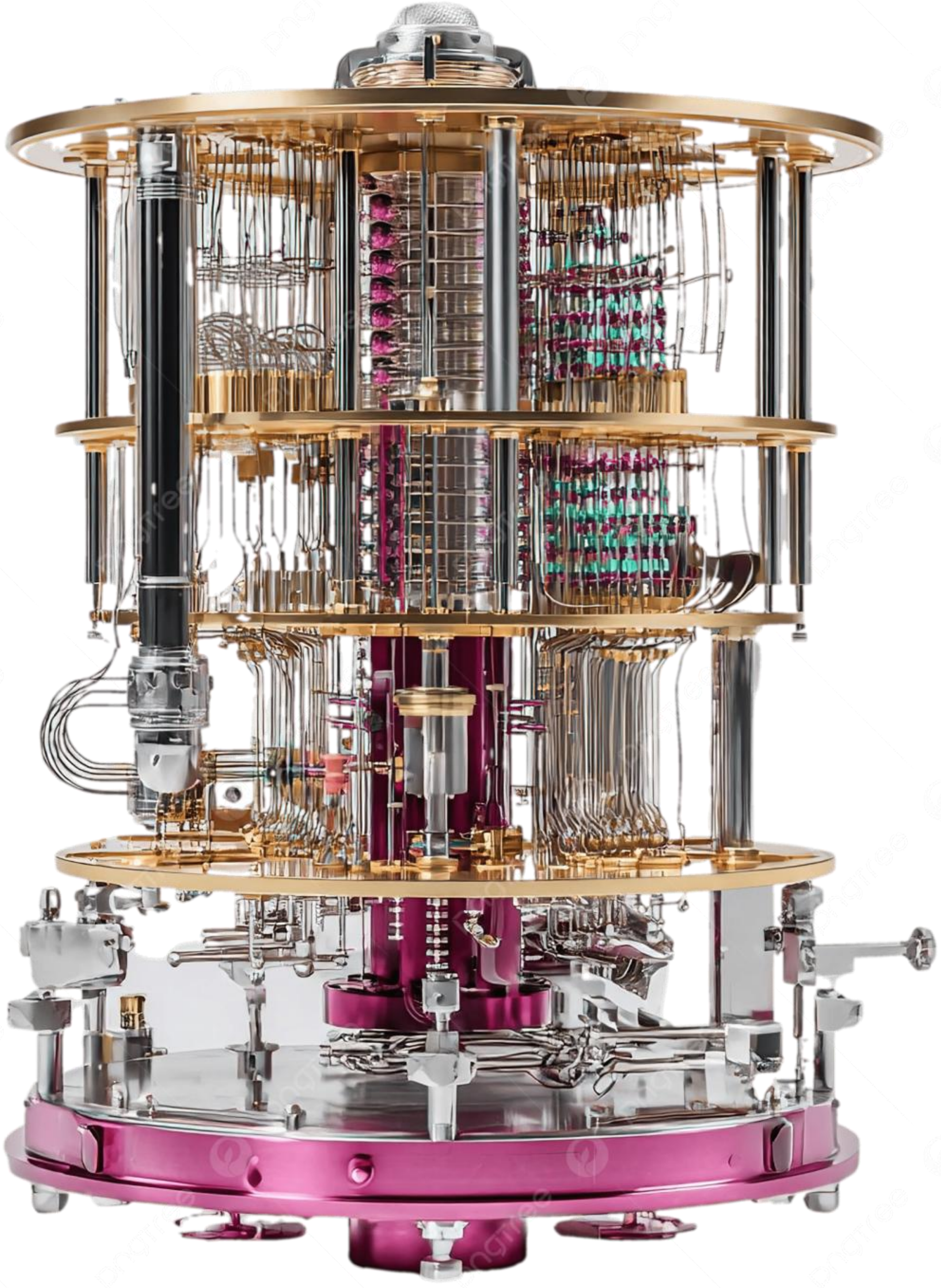
Universal Quantum

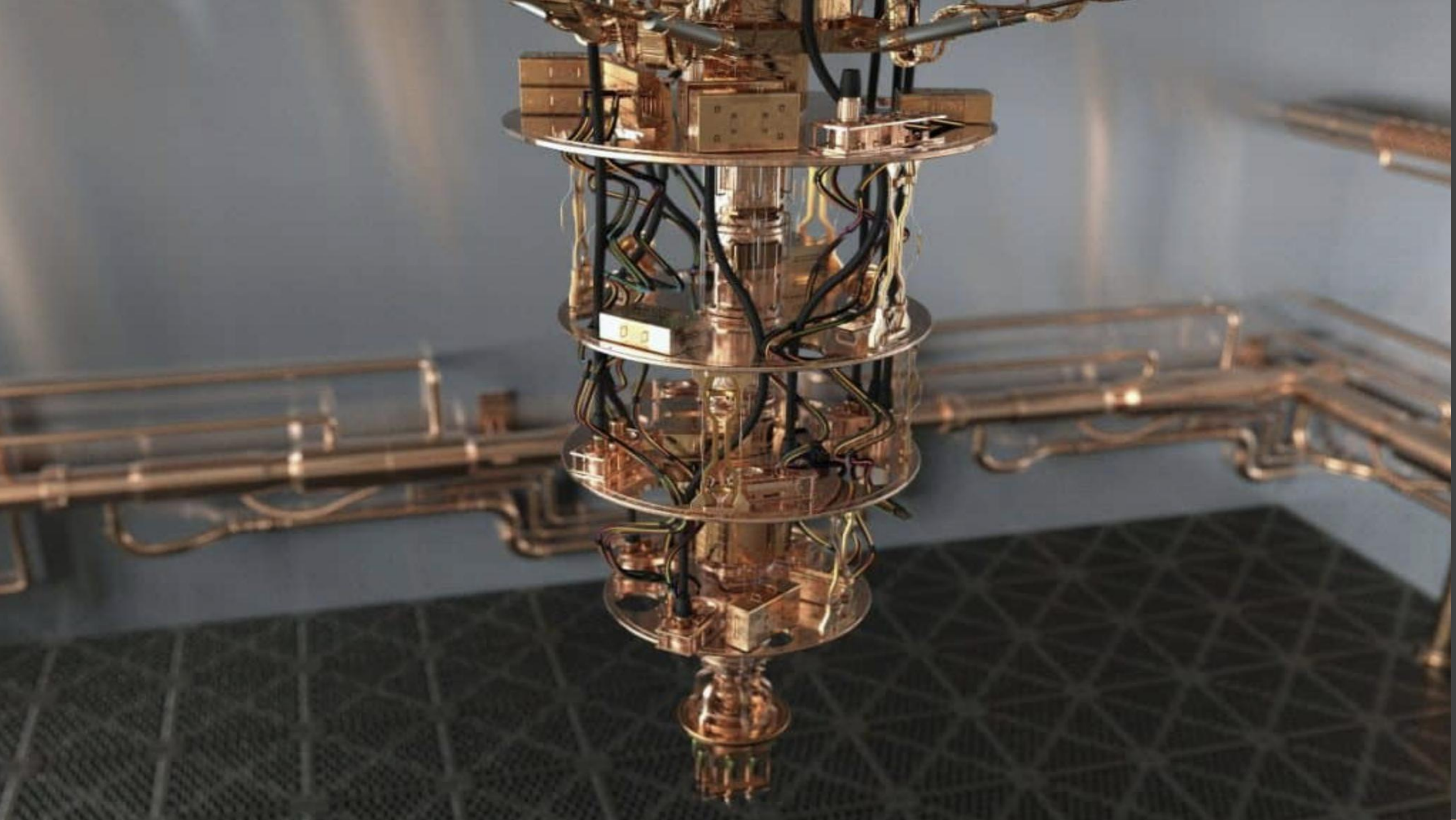
The universal quantum computer is the most powerful, the most general, and the hardest to build, posing a number of difficult technical challenges. Current estimates indicate that this machine will comprise more than 100,000 physical qubits.

APPLICATIONS
Secure computing
Machine Learning
Cryptography
Quantum Chemistry
Material Science
Optimization Problems
Sampling
Quantum Dynamics
Searching

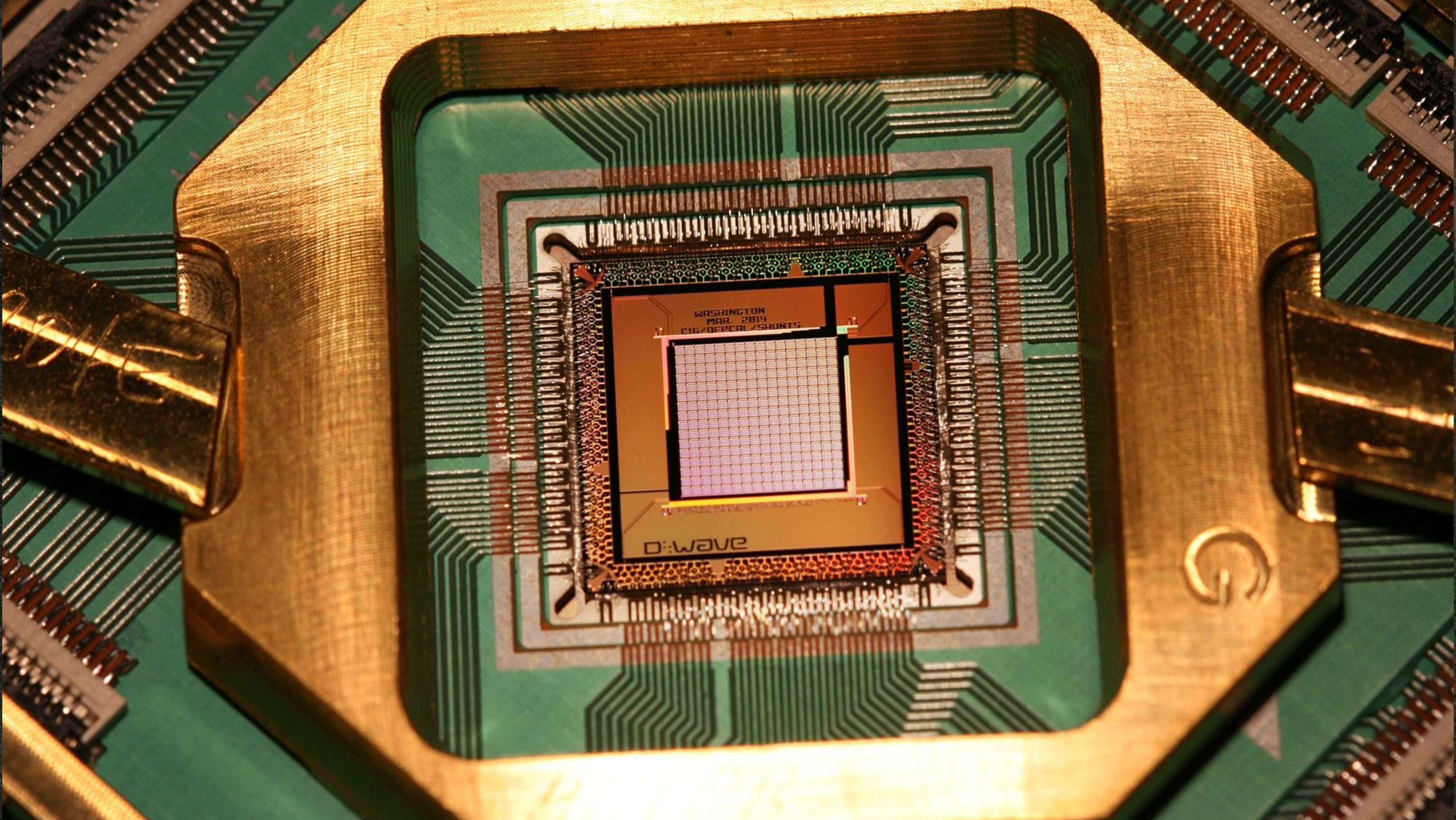
GENERALITY
Complete with known speed up

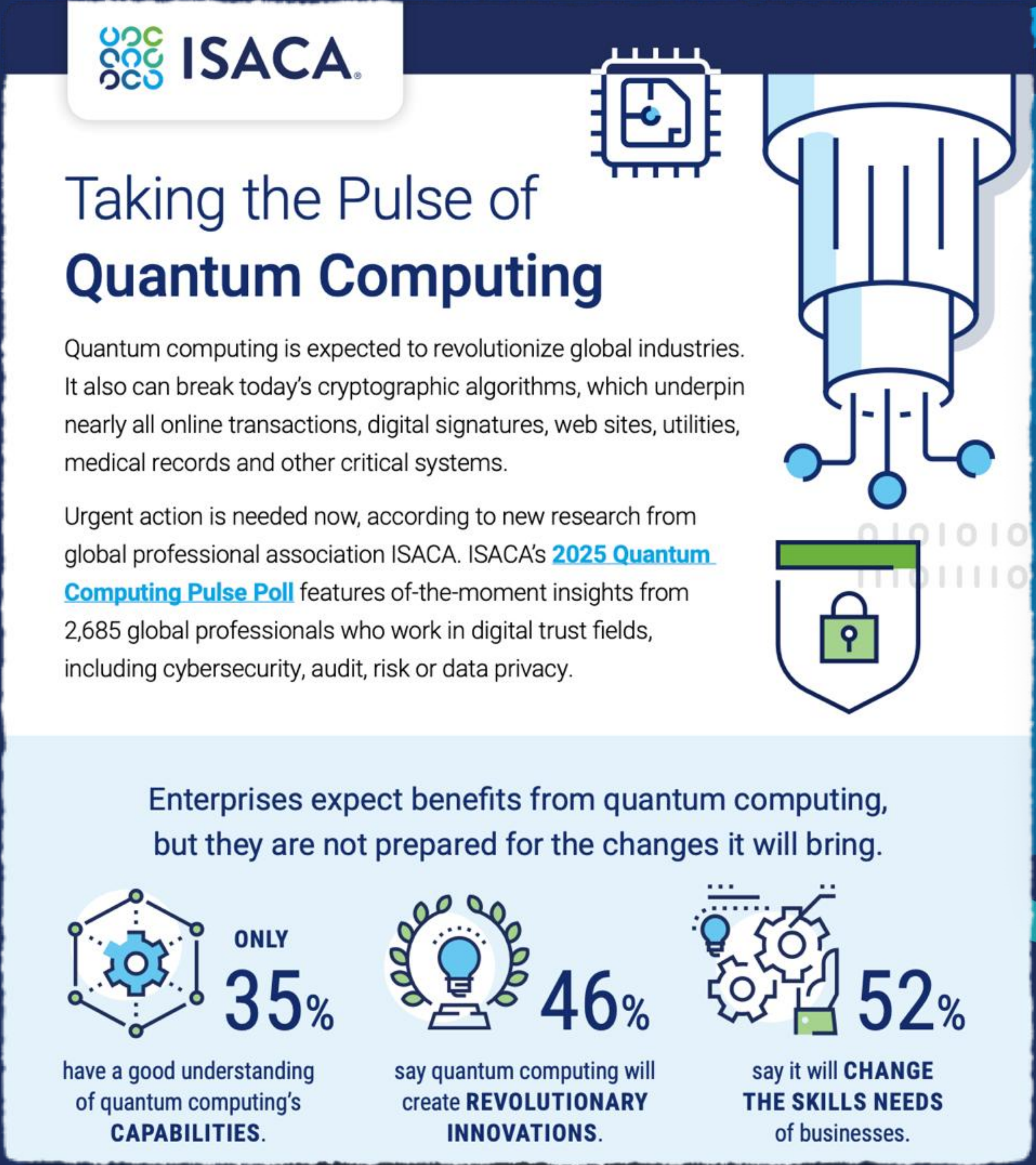
COMPUTATIONAL POWER
Very High





BSC
Barcelona
Supercomputing
Center


WASHINGTON
MAR. 2014
C16/OFPCAL/SHUNTS
D:WAVE



ISACA

Taking the Pulse of **Quantum Computing**

Quantum computing is expected to revolutionize global industries. It also can break today's cryptographic algorithms, which underpin nearly all online transactions, digital signatures, web sites, utilities, medical records and other critical systems.

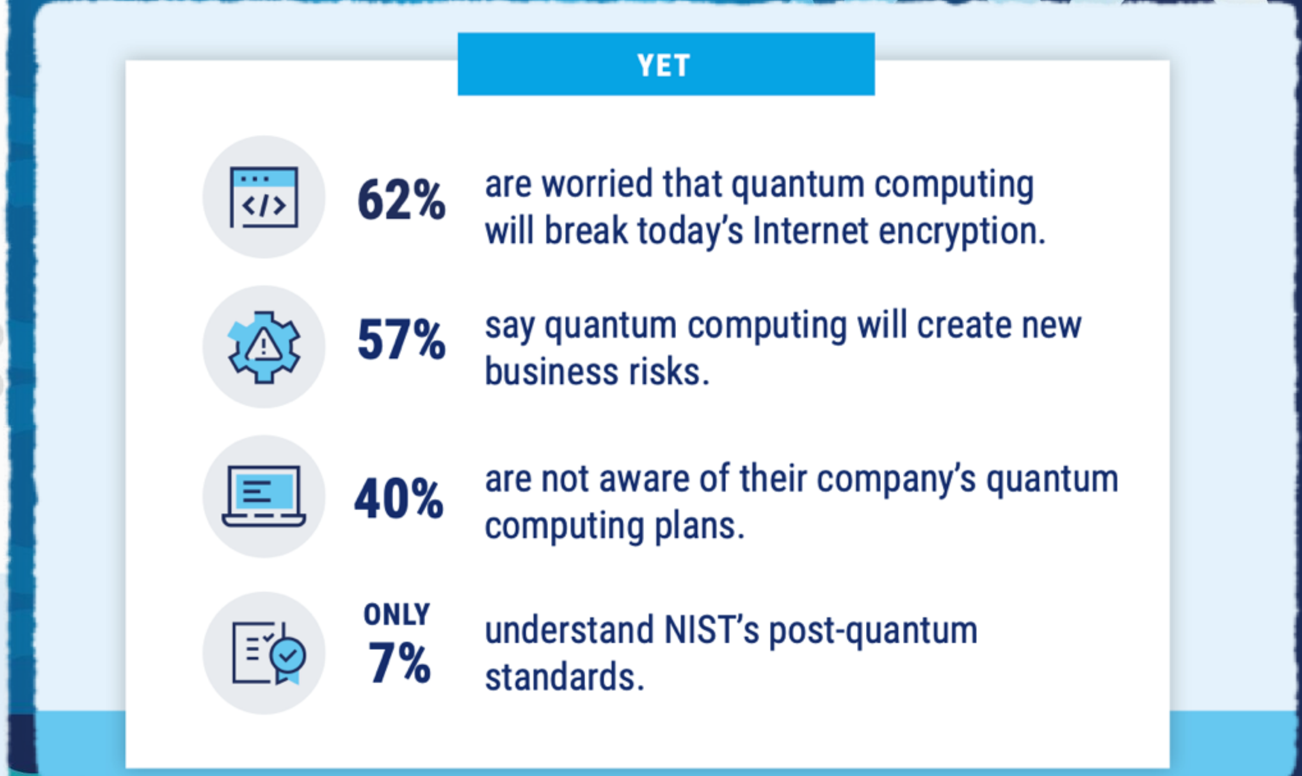
Urgent action is needed now, according to new research from global professional association ISACA. ISACA's **2025 Quantum Computing Pulse Poll** features of-the-moment insights from 2,685 global professionals who work in digital trust fields, including cybersecurity, audit, risk or data privacy.

Enterprises expect benefits from quantum computing, but they are not prepared for the changes it will bring.

ONLY **35%** have a good understanding of quantum computing's **CAPABILITIES**.

46% say quantum computing will create **REVOLUTIONARY INNOVATIONS**.

52% say it will **CHANGE THE SKILLS NEEDS** of businesses.



YET

62% are worried that quantum computing will break today's Internet encryption.

57% say quantum computing will create new business risks.

40% are not aware of their company's quantum computing plans.

ONLY 7% understand NIST's post-quantum standards.

ISACA

Cybercriminals are already collecting data to decrypt with quantum computing:

56%

are worried about "harvest now, decrypt later" attacks.

Many underestimate how quickly quantum computing may become widespread and break existing encryption.

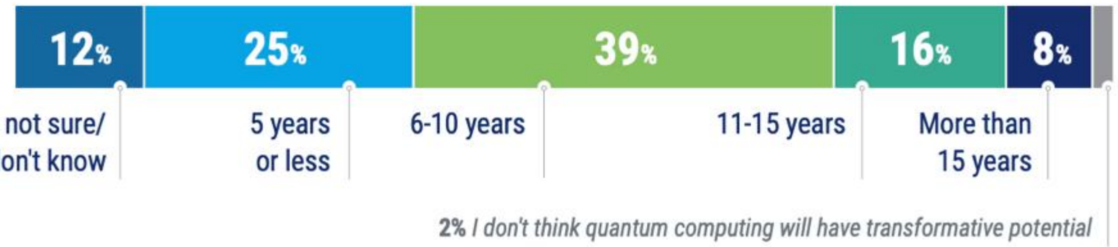
55%

have not taken steps to prepare for quantum computing.

Respondents are split on the expected time frame in which the full potential of quantum computing will be realized.

ONLY 5%

say it's a high business priority for the near future.



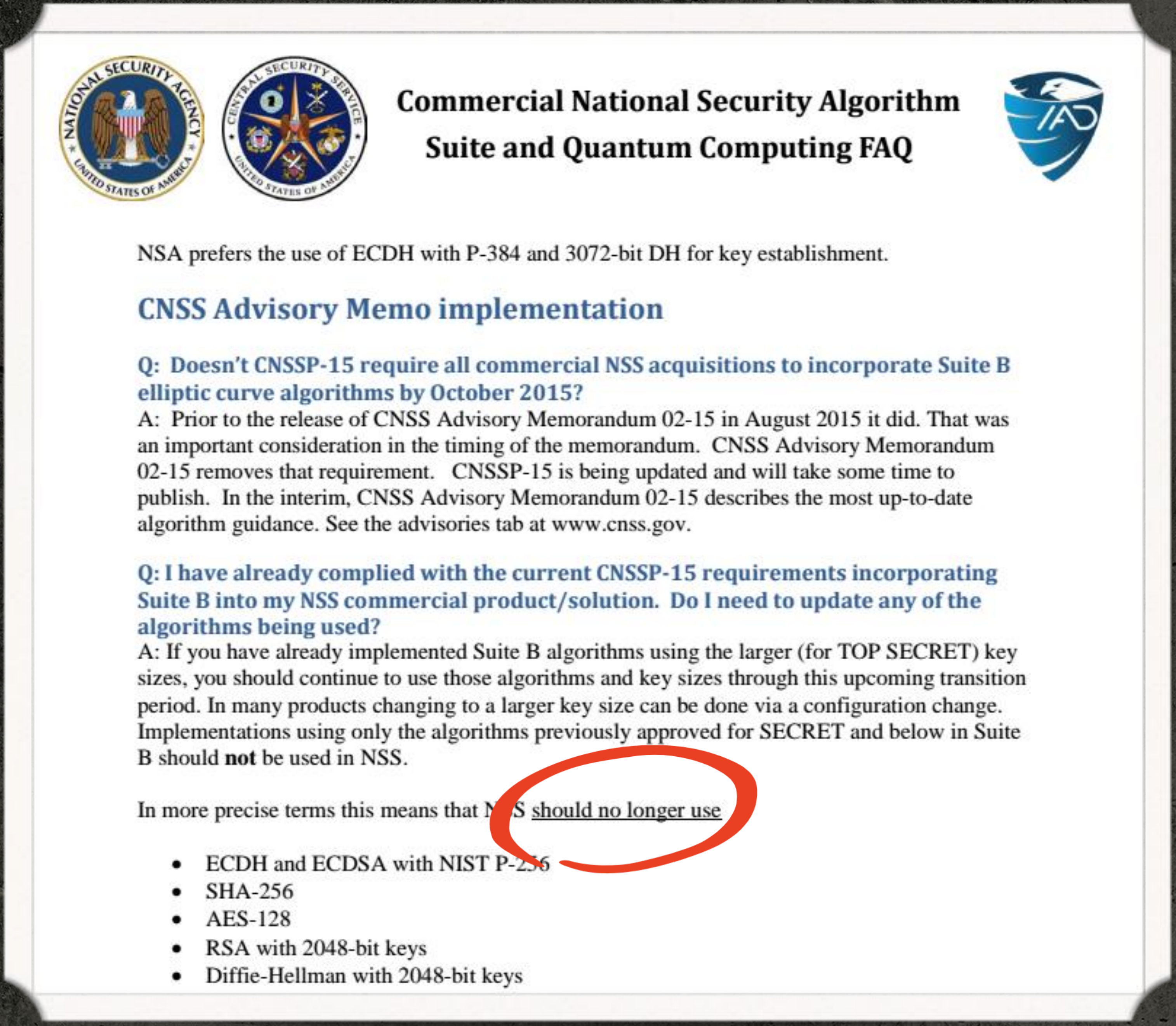
2% *I don't think quantum computing will have transformative potential*

IMMEDIATE ACTION REQUIRED

1. Educate stakeholders about quantum computing's risks and the urgent need for quantum-resistant encryption.
2. Assess and identify where encrypted data are stored; determine vulnerabilities.
3. Begin transitioning critical data and systems to quantum-resistant encryption.
4. Upgrade digital infrastructure, ensure all Internet-connected systems are secure.

For additional data points and analysis, visit www.isaca.org/quantum-pulse-poll

ISACA®



Commercial National Security Algorithm Suite and Quantum Computing FAQ

NSA prefers the use of ECDH with P-384 and 3072-bit DH for key establishment.

CNSS Advisory Memo implementation

Q: Doesn't CNSSP-15 require all commercial NSS acquisitions to incorporate Suite B elliptic curve algorithms by October 2015?

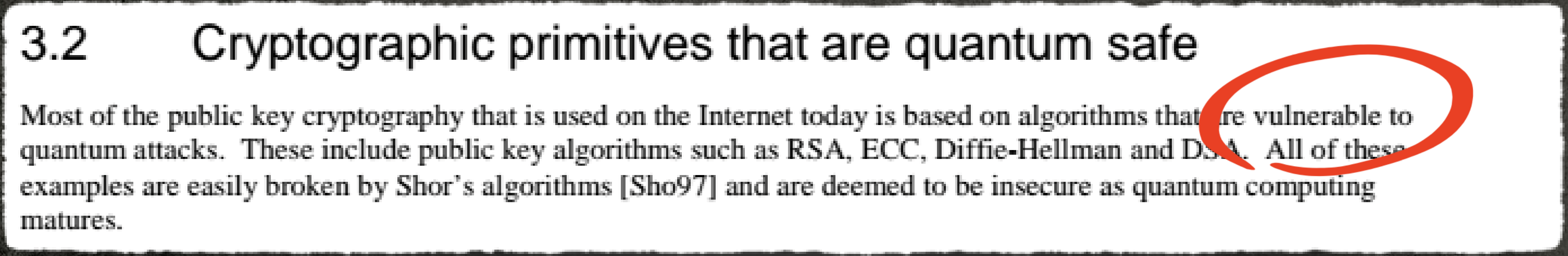
A: Prior to the release of CNSS Advisory Memorandum 02-15 in August 2015 it did. That was an important consideration in the timing of the memorandum. CNSS Advisory Memorandum 02-15 removes that requirement. CNSSP-15 is being updated and will take some time to publish. In the interim, CNSS Advisory Memorandum 02-15 describes the most up-to-date algorithm guidance. See the advisories tab at www.cnss.gov.

Q: I have already complied with the current CNSSP-15 requirements incorporating Suite B into my NSS commercial product/solution. Do I need to update any of the algorithms being used?

A: If you have already implemented Suite B algorithms using the larger (for TOP SECRET) key sizes, you should continue to use those algorithms and key sizes through this upcoming transition period. In many products changing to a larger key size can be done via a configuration change. Implementations using only the algorithms previously approved for SECRET and below in Suite B should **not** be used in NSS.

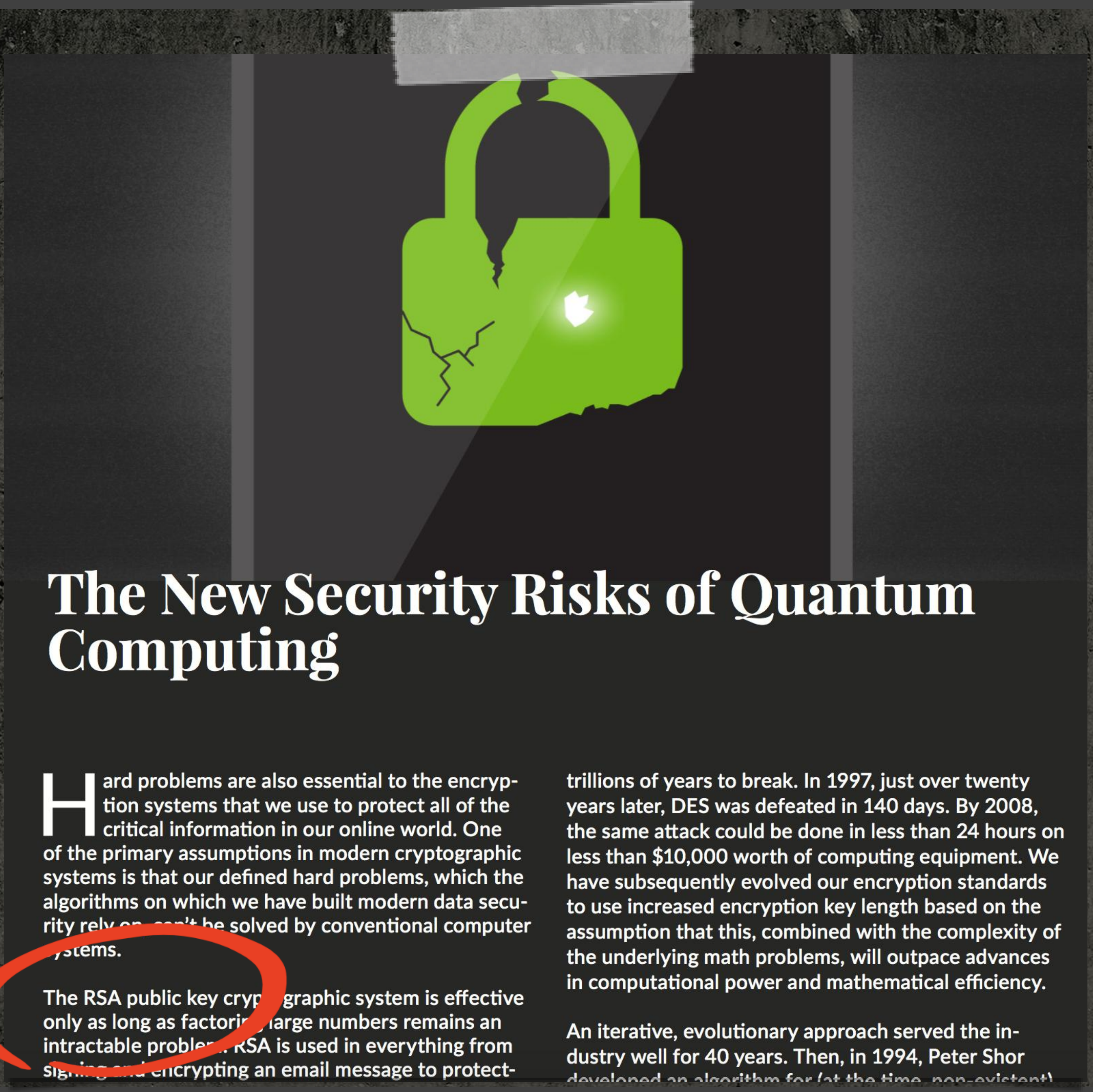
In more precise terms this means that NSS should no longer use

- ECDH and ECDSA with NIST P-256
- SHA-256
- AES-128
- RSA with 2048-bit keys
- Diffie-Hellman with 2048-bit keys



3.2 Cryptographic primitives that are quantum safe

Most of the public key cryptography that is used on the Internet today is based on algorithms that are vulnerable to quantum attacks. These include public key algorithms such as RSA, ECC, Diffie-Hellman and DSA. All of these examples are easily broken by Shor's algorithms [Sho97] and are deemed to be insecure as quantum computing matures.



The New Security Risks of Quantum Computing

Hard problems are also essential to the encryption systems that we use to protect all of the critical information in our online world. One of the primary assumptions in modern cryptographic systems is that our defined hard problems, which the algorithms on which we have built modern data security rely on, can't be solved by conventional computer systems.

The RSA public key cryptographic system is effective only as long as factoring large numbers remains an intractable problem. RSA is used in everything from signing and encrypting an email message to protect-

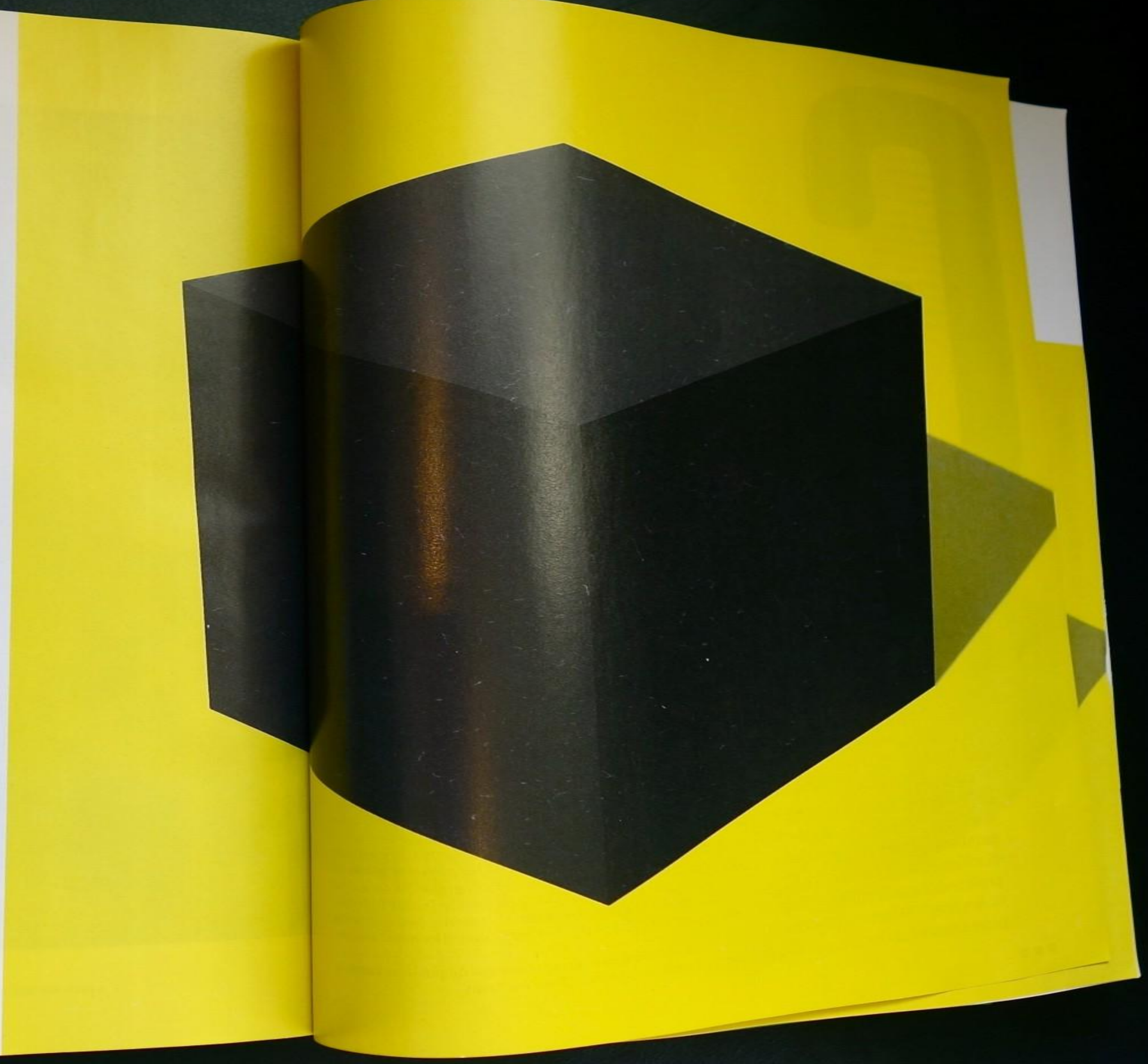
trillions of years to break. In 1997, just over twenty years later, DES was defeated in 140 days. By 2008, the same attack could be done in less than 24 hours on less than $10,000 worth of computing equipment. We have subsequently evolved our encryption standards to use increased encryption key length based on the assumption that this, combined with the complexity of the underlying math problems, will outpace advances in computational power and mathematical efficiency.

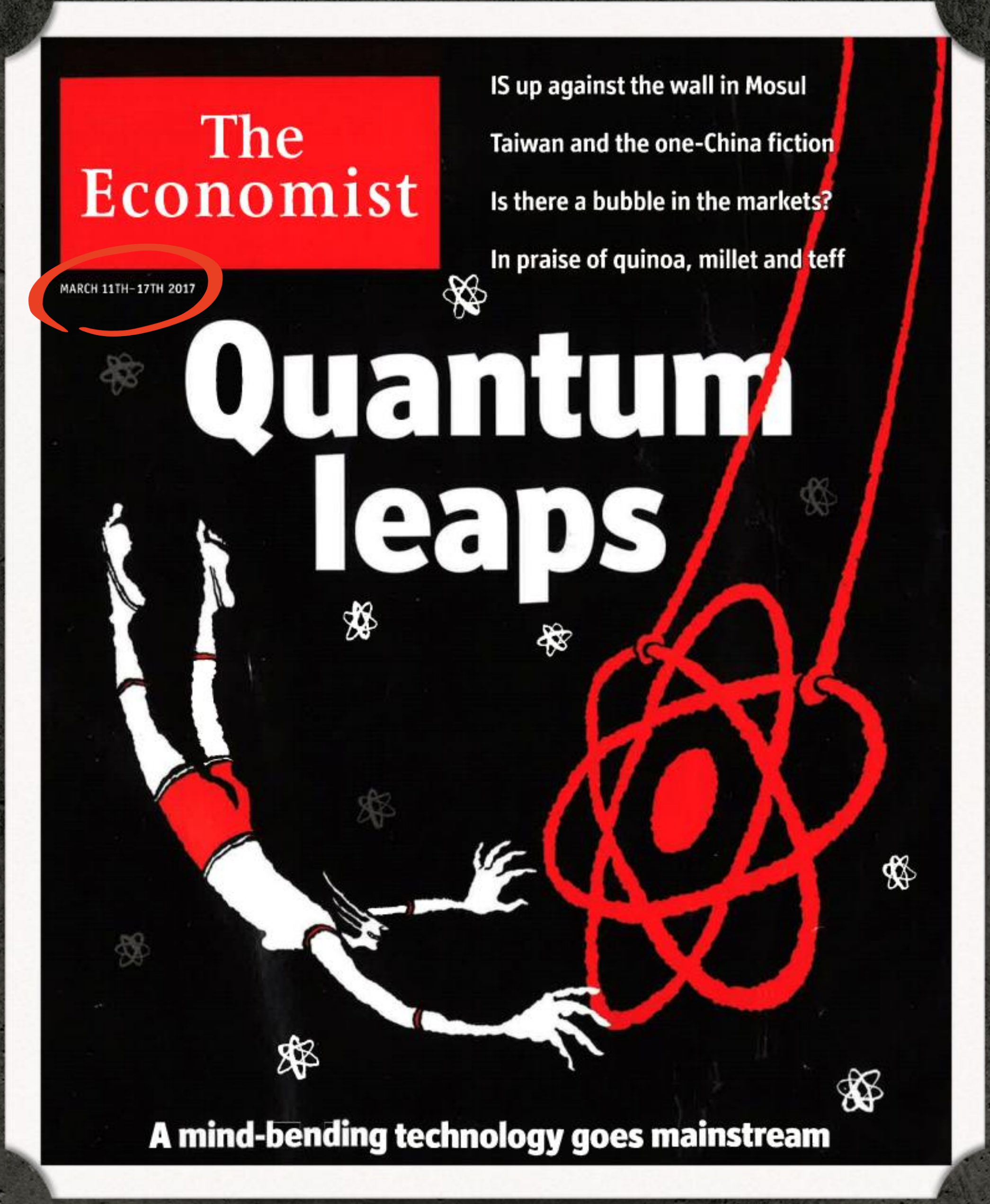
An iterative, evolutionary approach served the industry well for 40 years. Then, in 1994, Peter Shor developed an algorithm for (at the time, non-existent)

THE AGE OF QUANTUM COMPUTING HAS NOW ARRIVED

BY CLIVE THOMPSON

NAOYA FUJISHIRO





The Economist

MARCH 11TH–17TH 2017

IS up against the wall in Mosul

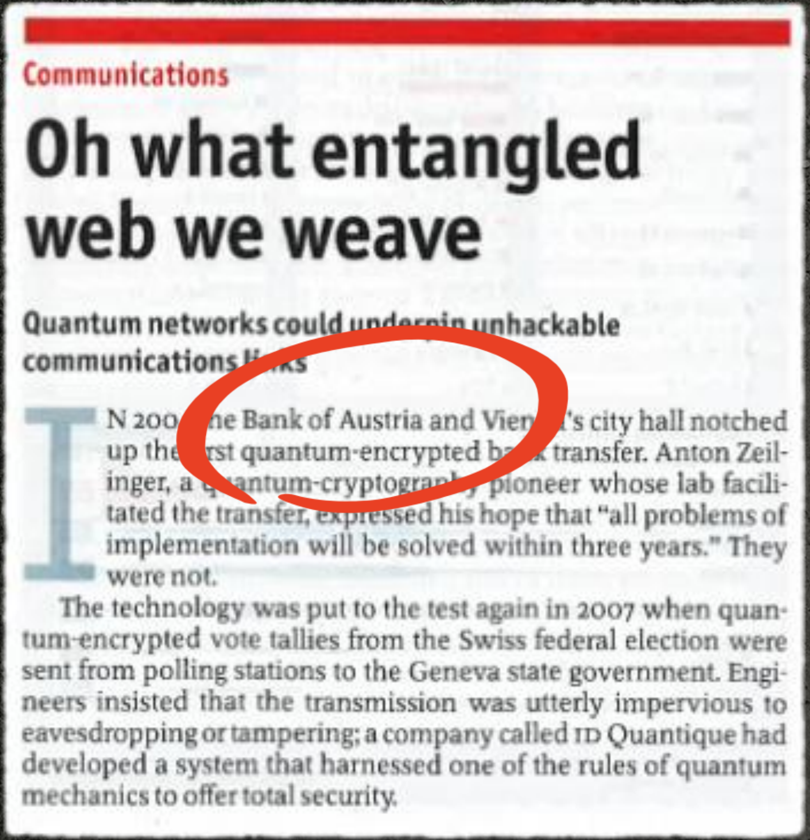
Taiwan and the one-China fiction

Is there a bubble in the markets?

In praise of quinoa, millet and teff

Quantum leaps

A mind-bending technology goes mainstream



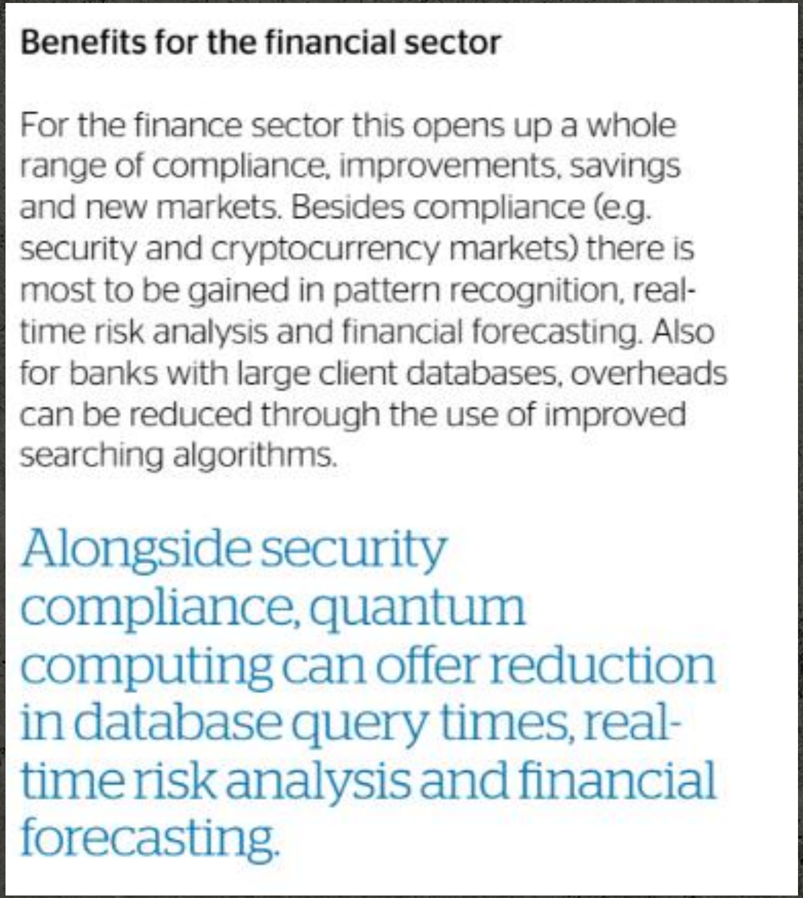
Communications

Oh what entangled web we weave

Quantum networks could underpin unhackable communications links

IN 2004 the Bank of Austria and Vienna's city hall notched up the first quantum-encrypted bank transfer. Anton Zeilinger, a quantum-cryptography pioneer whose lab facilitated the transfer, expressed his hope that "all problems of implementation will be solved within three years." They were not.

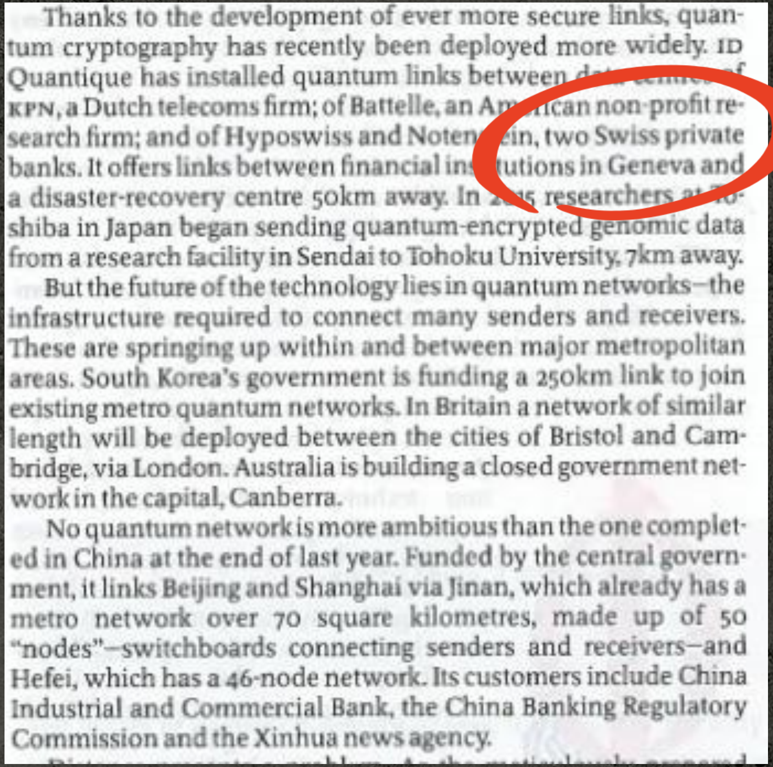
The technology was put to the test again in 2007 when quantum-encrypted vote tallies from the Swiss federal election were sent from polling stations to the Geneva state government. Engineers insisted that the transmission was utterly impervious to eavesdropping or tampering; a company called ID Quantique had developed a system that harnessed one of the rules of quantum mechanics to offer total security.



Benefits for the financial sector

For the finance sector this opens up a whole range of compliance, improvements, savings and new markets. Besides compliance (e.g. security and cryptocurrency markets) there is most to be gained in pattern recognition, real-time risk analysis and financial forecasting. Also for banks with large client databases, overheads can be reduced through the use of improved searching algorithms.

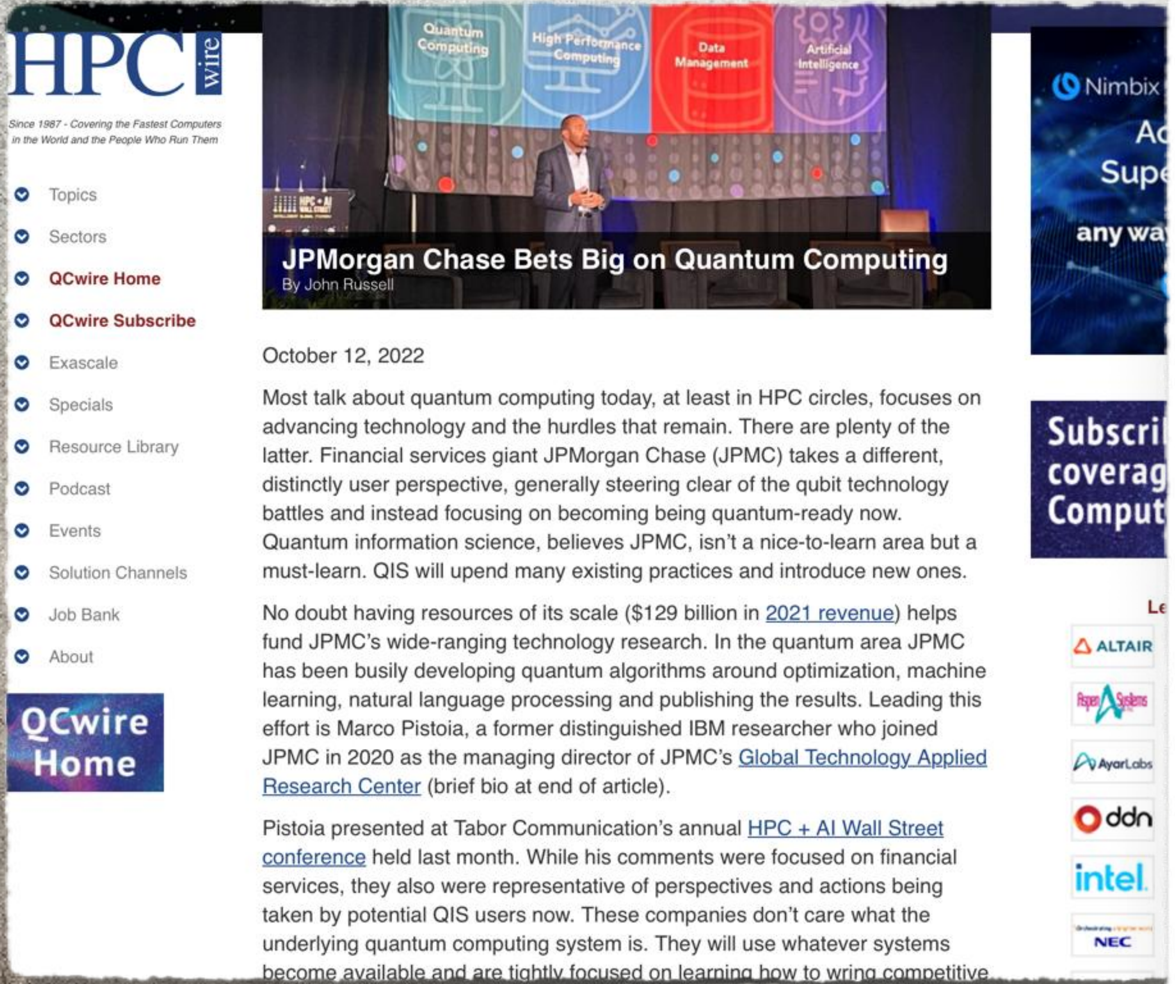
Alongside security compliance, quantum computing can offer reduction in database query times, real-time risk analysis and financial forecasting.



Thanks to the development of ever more secure links, quantum cryptography has recently been deployed more widely. ID Quantique has installed quantum links between data centres of KPN, a Dutch telecoms firm; of Battelle, an American non-profit research firm; and of Hyposwiss and Notenstein, two Swiss private banks. It offers links between financial institutions in Geneva and a disaster-recovery centre 50km away. In 2015 researchers at Toshiba in Japan began sending quantum-encrypted genomic data from a research facility in Sendai to Tohoku University, 7km away.

But the future of the technology lies in quantum networks—the infrastructure required to connect many senders and receivers. These are springing up within and between major metropolitan areas. South Korea's government is funding a 250km link to join existing metro quantum networks. In Britain a network of similar length will be deployed between the cities of Bristol and Cambridge, via London. Australia is building a closed government network in the capital, Canberra.

No quantum network is more ambitious than the one completed in China at the end of last year. Funded by the central government, it links Beijing and Shanghai via Jinan, which already has a metro network over 70 square kilometres, made up of 50 "nodes"—switchboards connecting senders and receivers—and Hefei, which has a 46-node network. Its customers include China Industrial and Commercial Bank, the China Banking Regulatory Commission and the Xinhua news agency.



HPCwire

Since 1987 - Covering the Fastest Computers in the World and the People Who Run Them

- Topics
- Sectors
- QCwire Home
- QCwire Subscribe
- Exascale
- Specials
- Resource Library
- Podcast
- Events
- Solution Channels
- Job Bank
- About

QCwire Home

JPMorgan Chase Bets Big on Quantum Computing

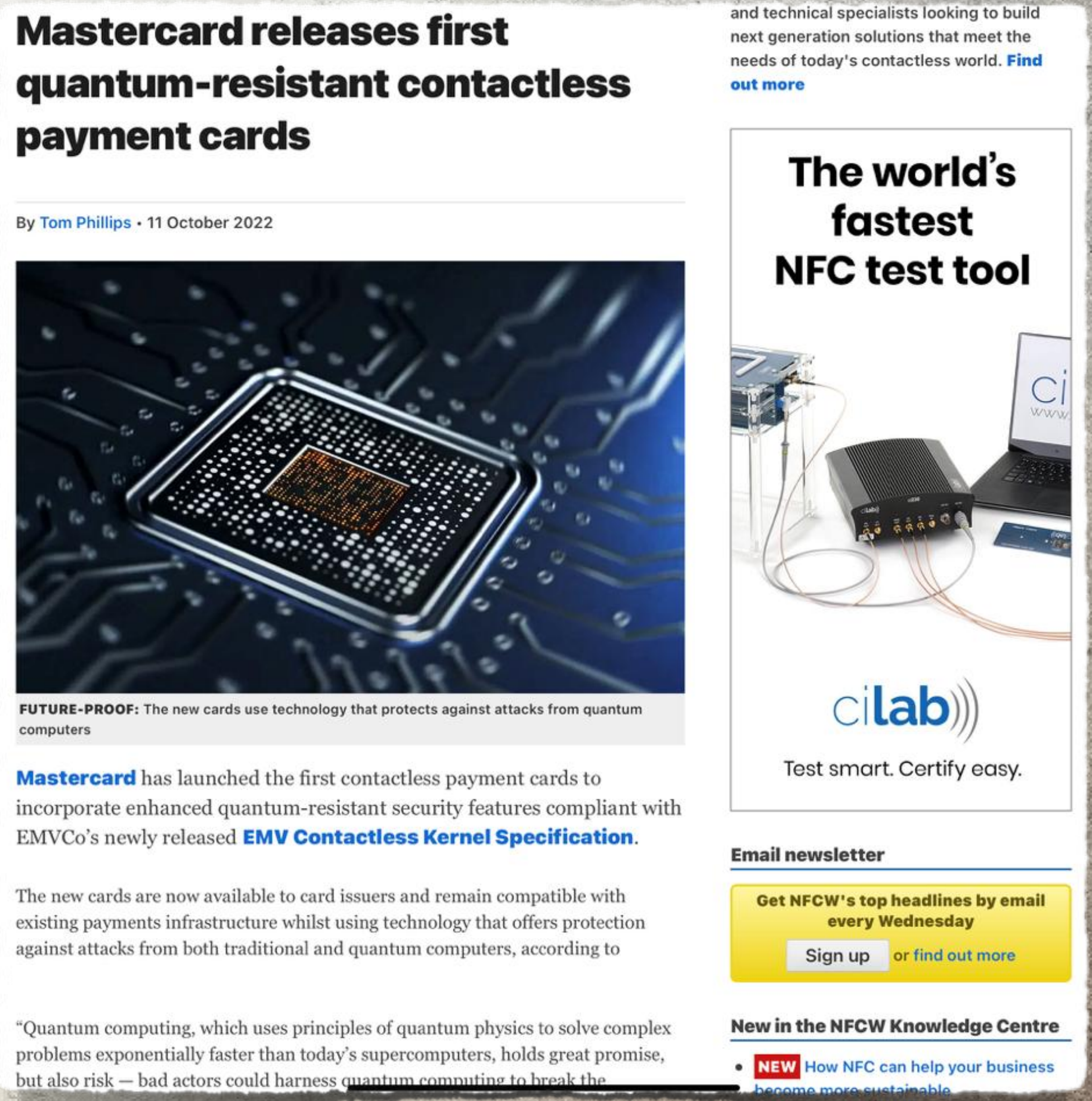
By John Russell

October 12, 2022

Most talk about quantum computing today, at least in HPC circles, focuses on advancing technology and the hurdles that remain. There are plenty of the latter. Financial services giant JPMorgan Chase (JPMC) takes a different, distinctly user perspective, generally steering clear of the qubit technology battles and instead focusing on becoming being quantum-ready now. Quantum information science, believes JPMC, isn't a nice-to-learn area but a must-learn. QIS will upend many existing practices and introduce new ones.

No doubt having resources of its scale ($129 billion in 2021 revenue) helps fund JPMC's wide-ranging technology research. In the quantum area JPMC has been busily developing quantum algorithms around optimization, machine learning, natural language processing and publishing the results. Leading this effort is Marco Pistoia, a former distinguished IBM researcher who joined JPMC in 2020 as the managing director of JPMC's Global Technology Applied Research Center (brief bio at end of article).

Pistoia presented at Tabor Communication's annual HPC + AI Wall Street conference held last month. While his comments were focused on financial services, they also were representative of perspectives and actions being taken by potential QIS users now. These companies don't care what the underlying quantum computing system is. They will use whatever systems become available and are tightly focused on learning how to wring competitive



Mastercard releases first quantum-resistant contactless payment cards

By Tom Phillips • 11 October 2022

FUTURE-PROOF: The new cards use technology that protects against attacks from quantum computers

Mastercard has launched the first contactless payment cards to incorporate enhanced quantum-resistant security features compliant with EMVCo's newly released EMV Contactless Kernel Specification.

The new cards are now available to card issuers and remain compatible with existing payments infrastructure whilst using technology that offers protection against attacks from both traditional and quantum computers, according to

"Quantum computing, which uses principles of quantum physics to solve complex problems exponentially faster than today's supercomputers, holds great promise, but also risk — bad actors could harness quantum computing to break the

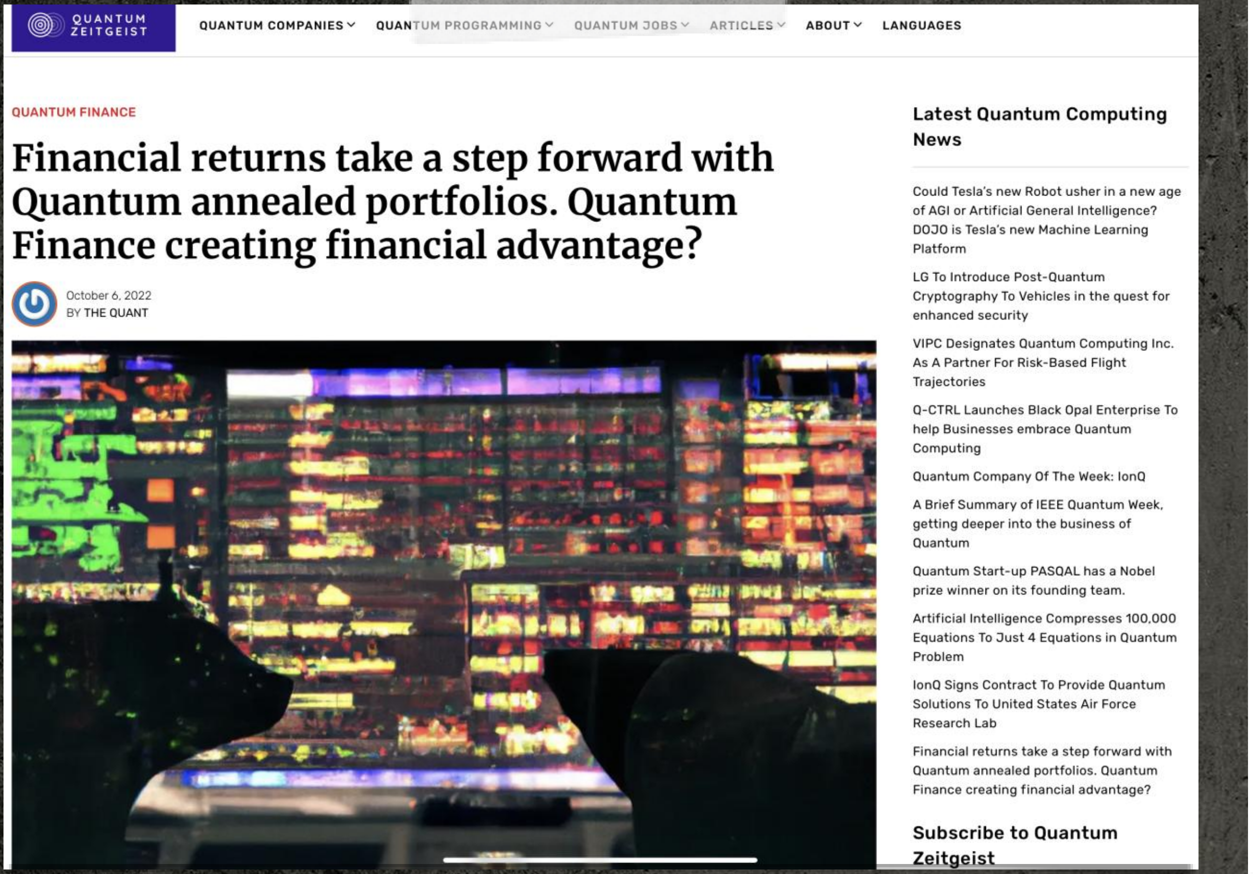
Email newsletter

Get NFCW's top headlines by email every Wednesday

Sign up or find out more

New in the NFCW Knowledge Centre

- NEW How NFC can help your business become more sustainable



QUANTUM FINANCE

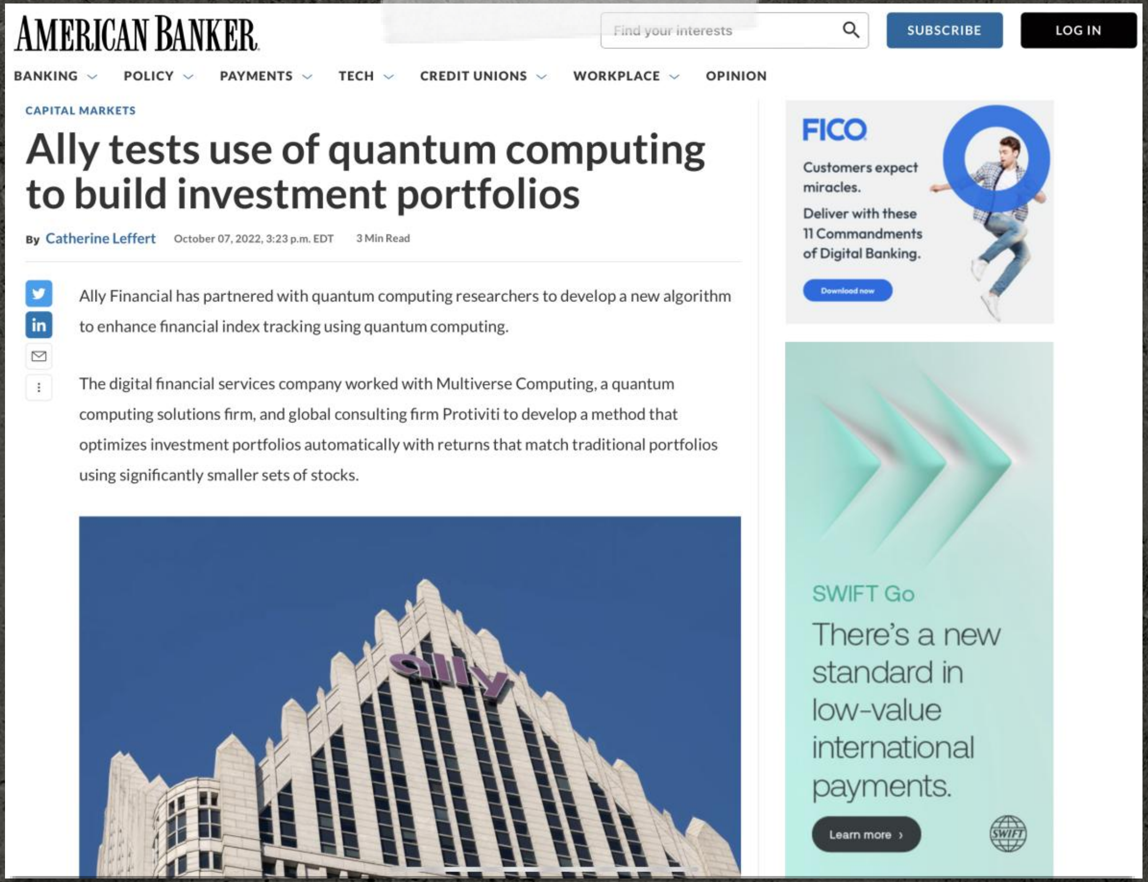
Financial returns take a step forward with Quantum annealed portfolios. Quantum Finance creating financial advantage?

October 6, 2022
BY THE QUANT

Latest Quantum Computing News

- Could Tesla's new Robot usher in a new age of AGI or Artificial General Intelligence? DOJO is Tesla's new Machine Learning Platform
- LG To Introduce Post-Quantum Cryptography To Vehicles in the quest for enhanced security
- VIPC Designates Quantum Computing Inc. As A Partner For Risk-Based Flight Trajectories
- Q-CTRL Launches Black Opal Enterprise To help Businesses embrace Quantum Computing
- Quantum Company Of The Week: IonQ
- A Brief Summary of IEEE Quantum Week, getting deeper into the business of Quantum
- Quantum Start-up PASQAL has a Nobel prize winner on its founding team.
- Artificial Intelligence Compresses 100,000 Equations To Just 4 Equations in Quantum Problem
- IonQ Signs Contract To Provide Quantum Solutions To United States Air Force Research Lab
- Financial returns take a step forward with Quantum annealed portfolios. Quantum Finance creating financial advantage?

Subscribe to Quantum Zeitgeist



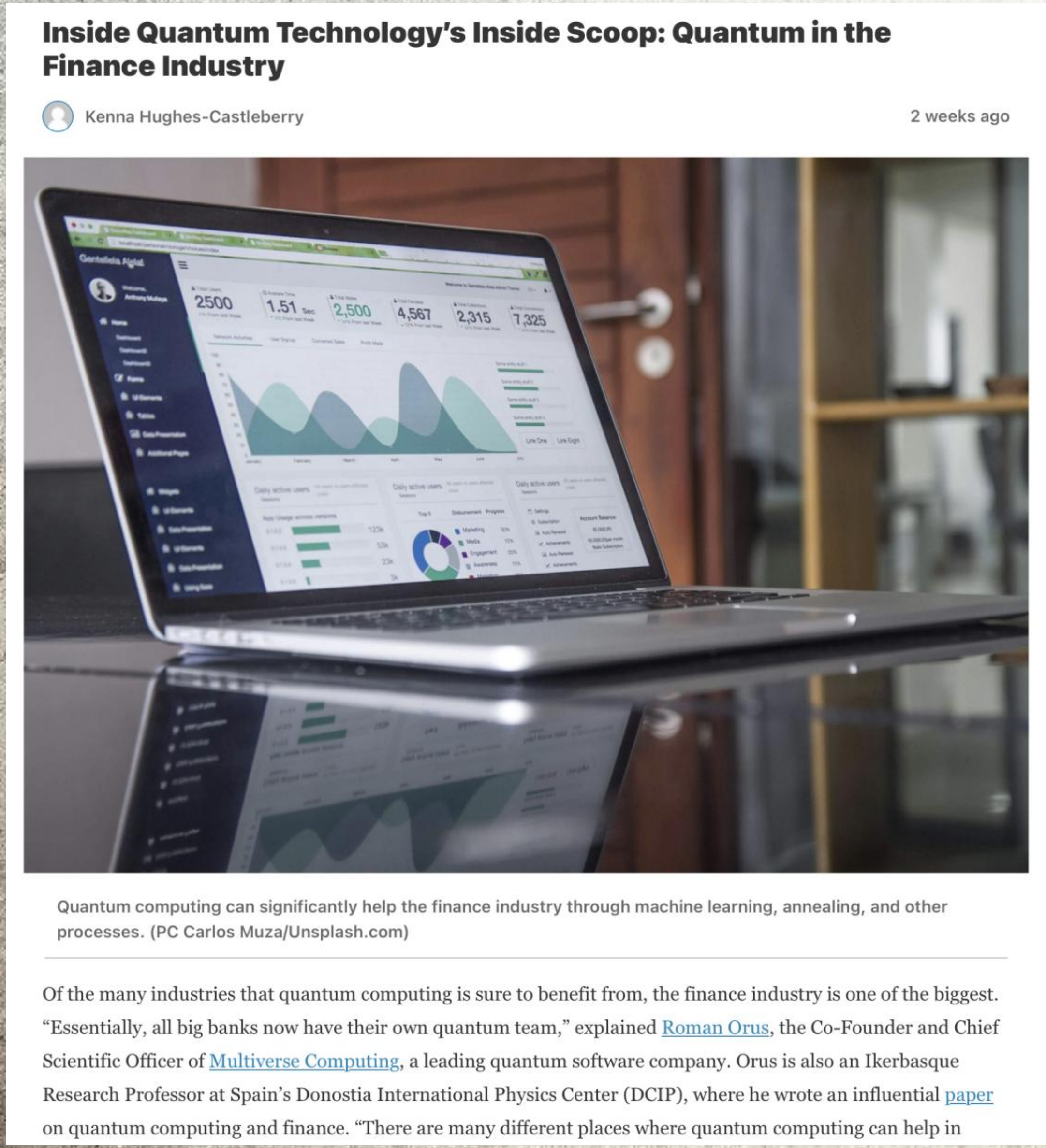
CAPITAL MARKETS

Ally tests use of quantum computing to build investment portfolios

By Catherine Leffert October 07, 2022, 3:23 p.m. EDT 3 Min Read

Ally Financial has partnered with quantum computing researchers to develop a new algorithm to enhance financial index tracking using quantum computing.

The digital financial services company worked with Multiverse Computing, a quantum computing solutions firm, and global consulting firm Protiviti to develop a method that optimizes investment portfolios automatically with returns that match traditional portfolios using significantly smaller sets of stocks.



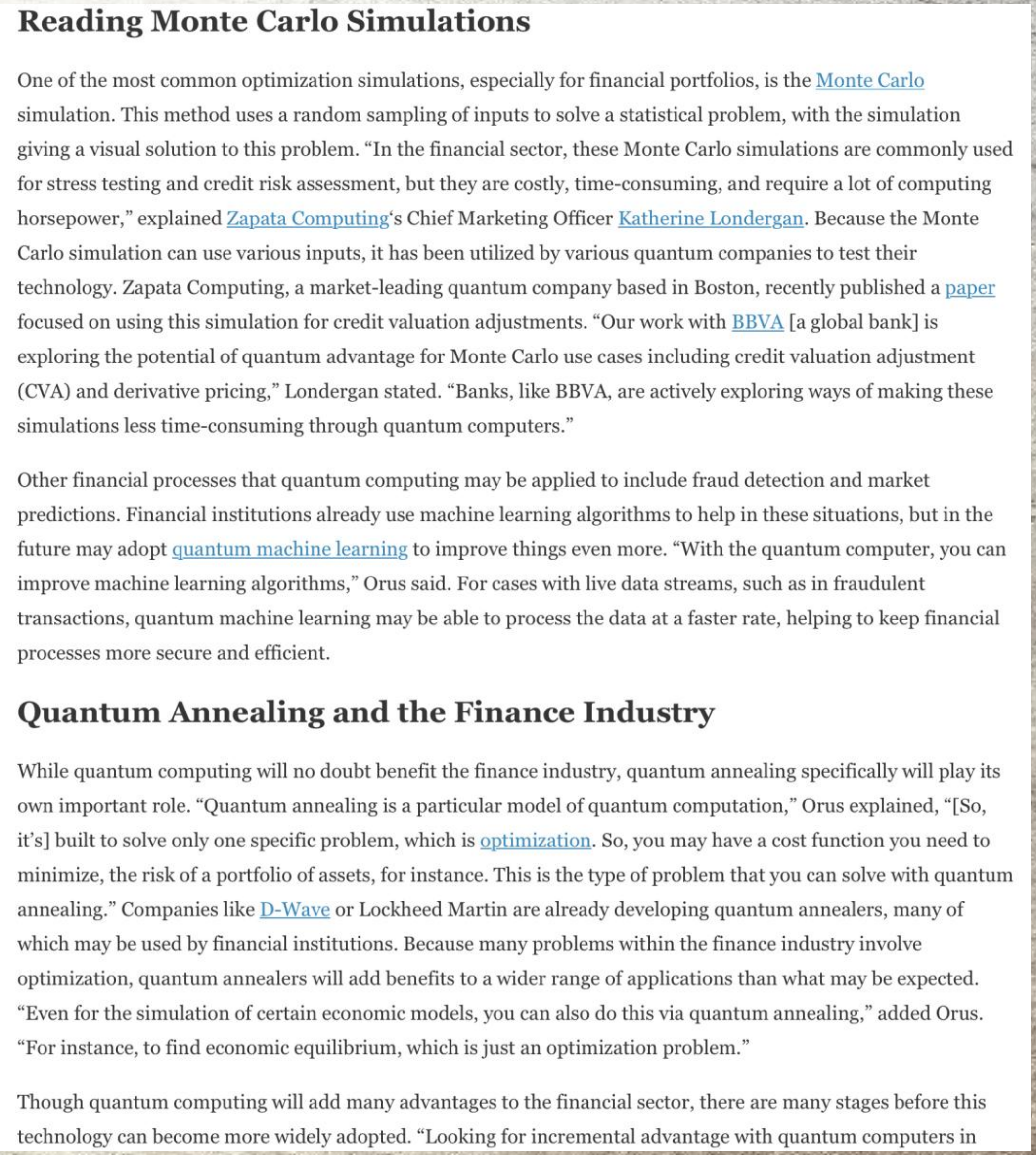
Inside Quantum Technology's Inside Scoop: Quantum in the Finance Industry

Kenna Hughes-Castleberry

2 weeks ago

Quantum computing can significantly help the finance industry through machine learning, annealing, and other processes. (PC Carlos Muza/Unsplash.com)

Of the many industries that quantum computing is sure to benefit from, the finance industry is one of the biggest. "Essentially, all big banks now have their own quantum team," explained Roman Orus, the Co-Founder and Chief Scientific Officer of Multiverse Computing, a leading quantum software company. Orus is also an Ikerbasque Research Professor at Spain's Donostia International Physics Center (DCIP), where he wrote an influential paper on quantum computing and finance. "There are many different places where quantum computing can help in



Reading Monte Carlo Simulations

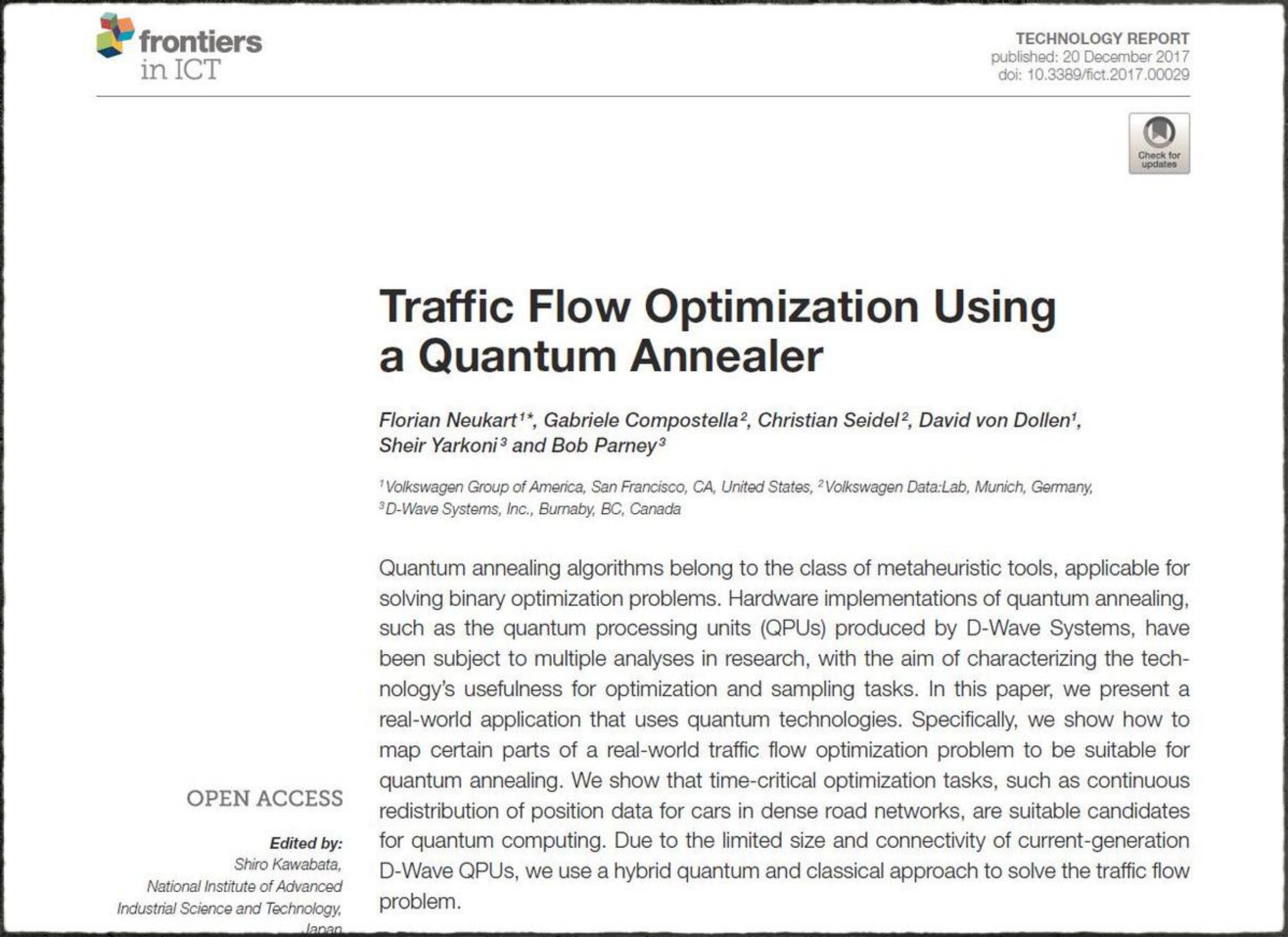
One of the most common optimization simulations, especially for financial portfolios, is the Monte Carlo simulation. This method uses a random sampling of inputs to solve a statistical problem, with the simulation giving a visual solution to this problem. "In the financial sector, these Monte Carlo simulations are commonly used for stress testing and credit risk assessment, but they are costly, time-consuming, and require a lot of computing horsepower," explained Zapata Computing's Chief Marketing Officer Katherine Londergan. Because the Monte Carlo simulation can use various inputs, it has been utilized by various quantum companies to test their technology. Zapata Computing, a market-leading quantum company based in Boston, recently published a paper focused on using this simulation for credit valuation adjustments. "Our work with BBVA [a global bank] is exploring the potential of quantum advantage for Monte Carlo use cases including credit valuation adjustment (CVA) and derivative pricing," Londergan stated. "Banks, like BBVA, are actively exploring ways of making these simulations less time-consuming through quantum computers."

Other financial processes that quantum computing may be applied to include fraud detection and market predictions. Financial institutions already use machine learning algorithms to help in these situations, but in the future may adopt quantum machine learning to improve things even more. "With the quantum computer, you can improve machine learning algorithms," Orus said. For cases with live data streams, such as in fraudulent transactions, quantum machine learning may be able to process the data at a faster rate, helping to keep financial processes more secure and efficient.

Quantum Annealing and the Finance Industry

While quantum computing will no doubt benefit the finance industry, quantum annealing specifically will play its own important role. "Quantum annealing is a particular model of quantum computation," Orus explained, "[So, it's] built to solve only one specific problem, which is optimization. So, you may have a cost function you need to minimize, the risk of a portfolio of assets, for instance. This is the type of problem that you can solve with quantum annealing." Companies like D-Wave or Lockheed Martin are already developing quantum annealers, many of which may be used by financial institutions. Because many problems within the finance industry involve optimization, quantum annealers will add benefits to a wider range of applications than what may be expected. "Even for the simulation of certain economic models, you can also do this via quantum annealing," added Orus. "For instance, to find economic equilibrium, which is just an optimization problem."

Though quantum computing will add many advantages to the financial sector, there are many stages before this technology can become more widely adopted. "Looking for incremental advantage with quantum computers in



frontiers in ICT

TECHNOLOGY REPORT
published: 20 December 2017
doi: 10.3389/fict.2017.00029

Check for updates

Traffic Flow Optimization Using a Quantum Annealer

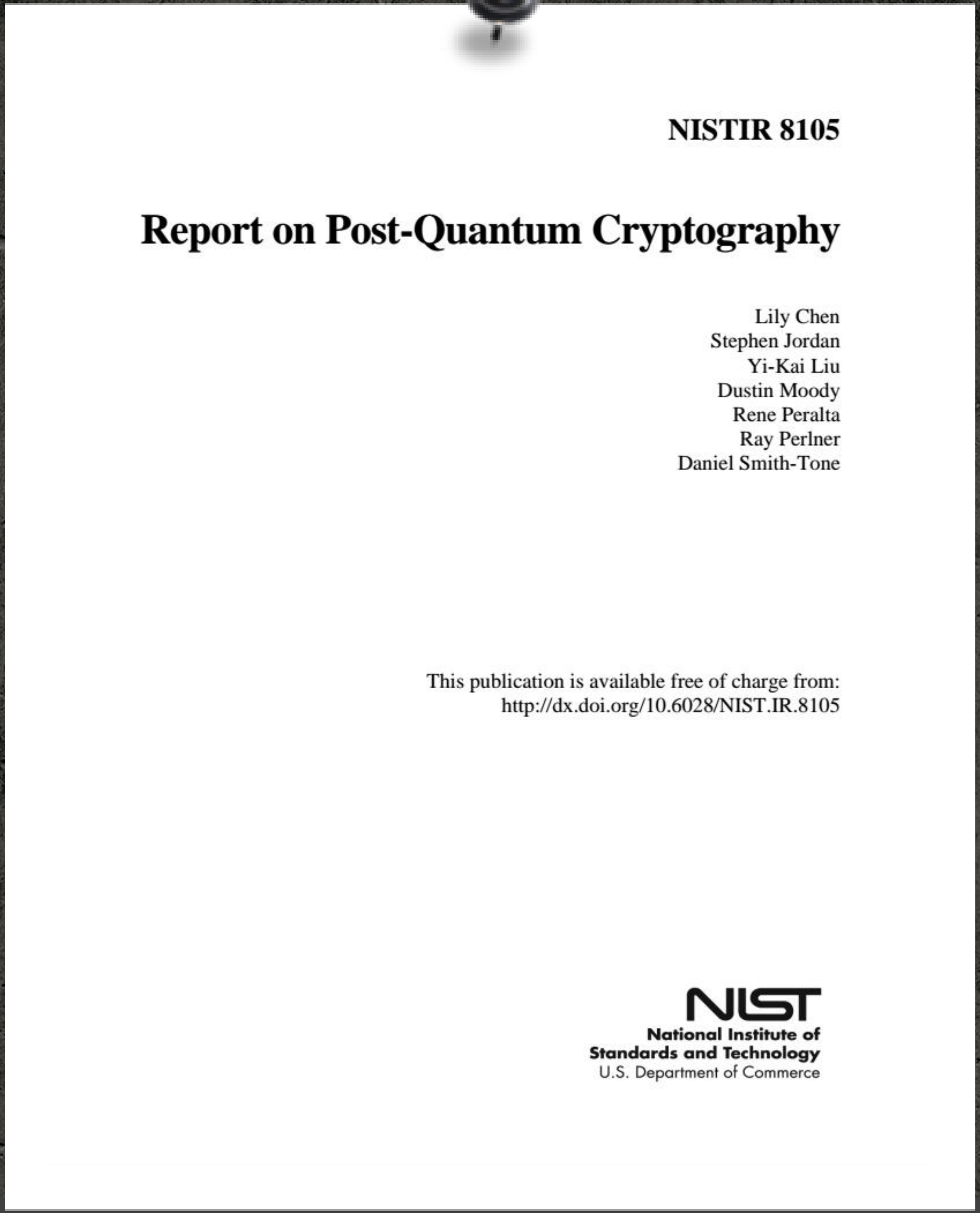
Florian Neukart[1]*, *Gabriele Compostella*[2], *Christian Seidel*[2], *David von Dollen*[1], *Sheir Yarkoni*[3] *and Bob Parney*[3]

[1] *Volkswagen Group of America, San Francisco, CA, United States,* [2] *Volkswagen Data:Lab, Munich, Germany,* [3] *D-Wave Systems, Inc., Burnaby, BC, Canada*

Quantum annealing algorithms belong to the class of metaheuristic tools, applicable for solving binary optimization problems. Hardware implementations of quantum annealing, such as the quantum processing units (QPUs) produced by D-Wave Systems, have been subject to multiple analyses in research, with the aim of characterizing the technology's usefulness for optimization and sampling tasks. In this paper, we present a real-world application that uses quantum technologies. Specifically, we show how to map certain parts of a real-world traffic flow optimization problem to be suitable for quantum annealing. We show that time-critical optimization tasks, such as continuous redistribution of position data for cars in dense road networks, are suitable candidates for quantum computing. Due to the limited size and connectivity of current-generation D-Wave QPUs, we use a hybrid quantum and classical approach to solve the traffic flow problem.

OPEN ACCESS

Edited by:
Shiro Kawabata,
National Institute of Advanced
Industrial Science and Technology,
Japan



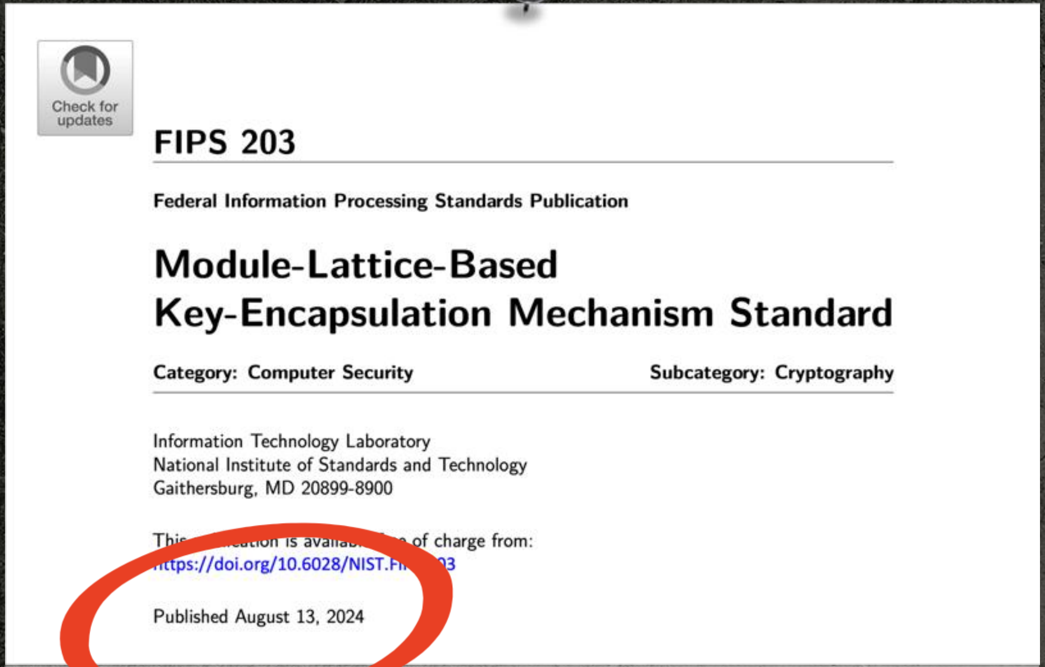
NISTIR 8105

Report on Post-Quantum Cryptography

Lily Chen
Stephen Jordan
Yi-Kai Liu
Dustin Moody
Rene Peralta
Ray Perlner
Daniel Smith-Tone

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8105

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



Check for updates

FIPS 203

Federal Information Processing Standards Publication

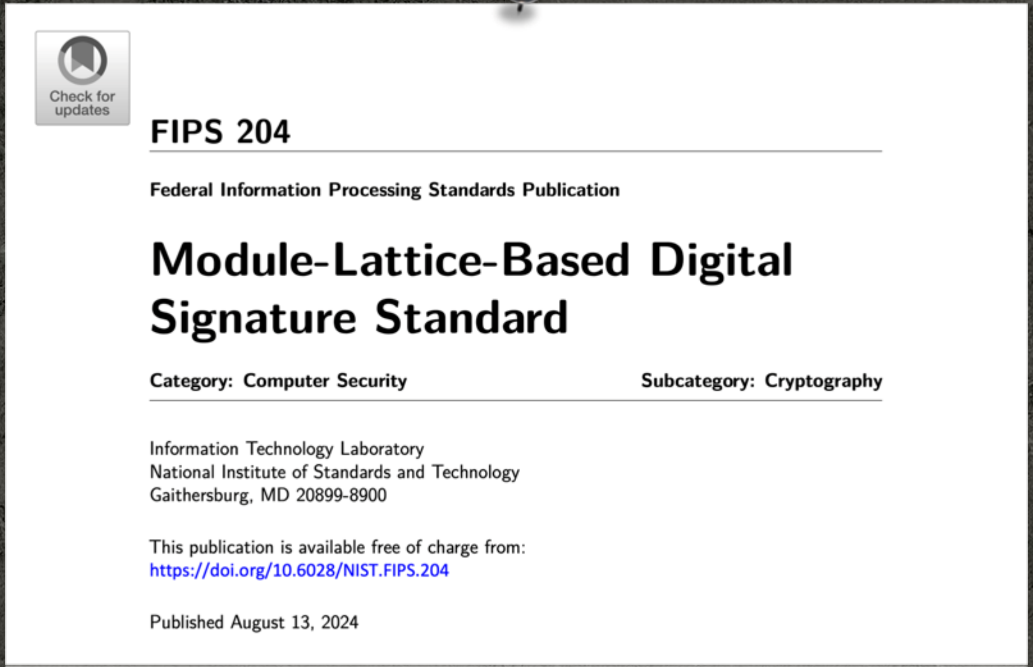
Module-Lattice-Based Key-Encapsulation Mechanism Standard

Category: Computer Security Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203

Published August 13, 2024



Check for updates

FIPS 204

Federal Information Processing Standards Publication

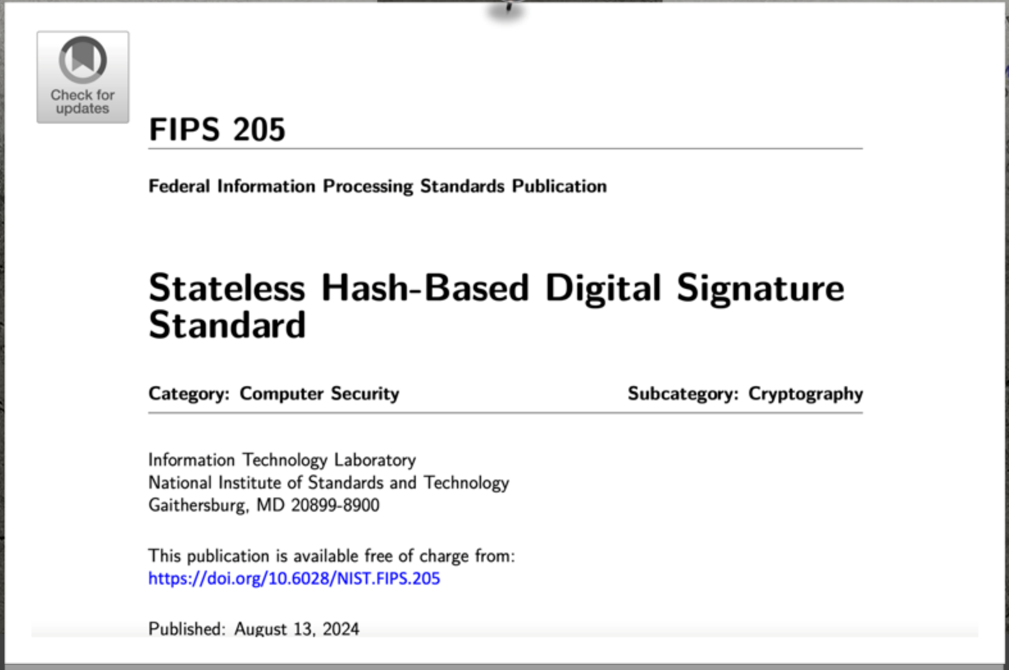
Module-Lattice-Based Digital Signature Standard

Category: Computer Security Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.204

Published August 13, 2024



Check for updates

FIPS 205

Federal Information Processing Standards Publication

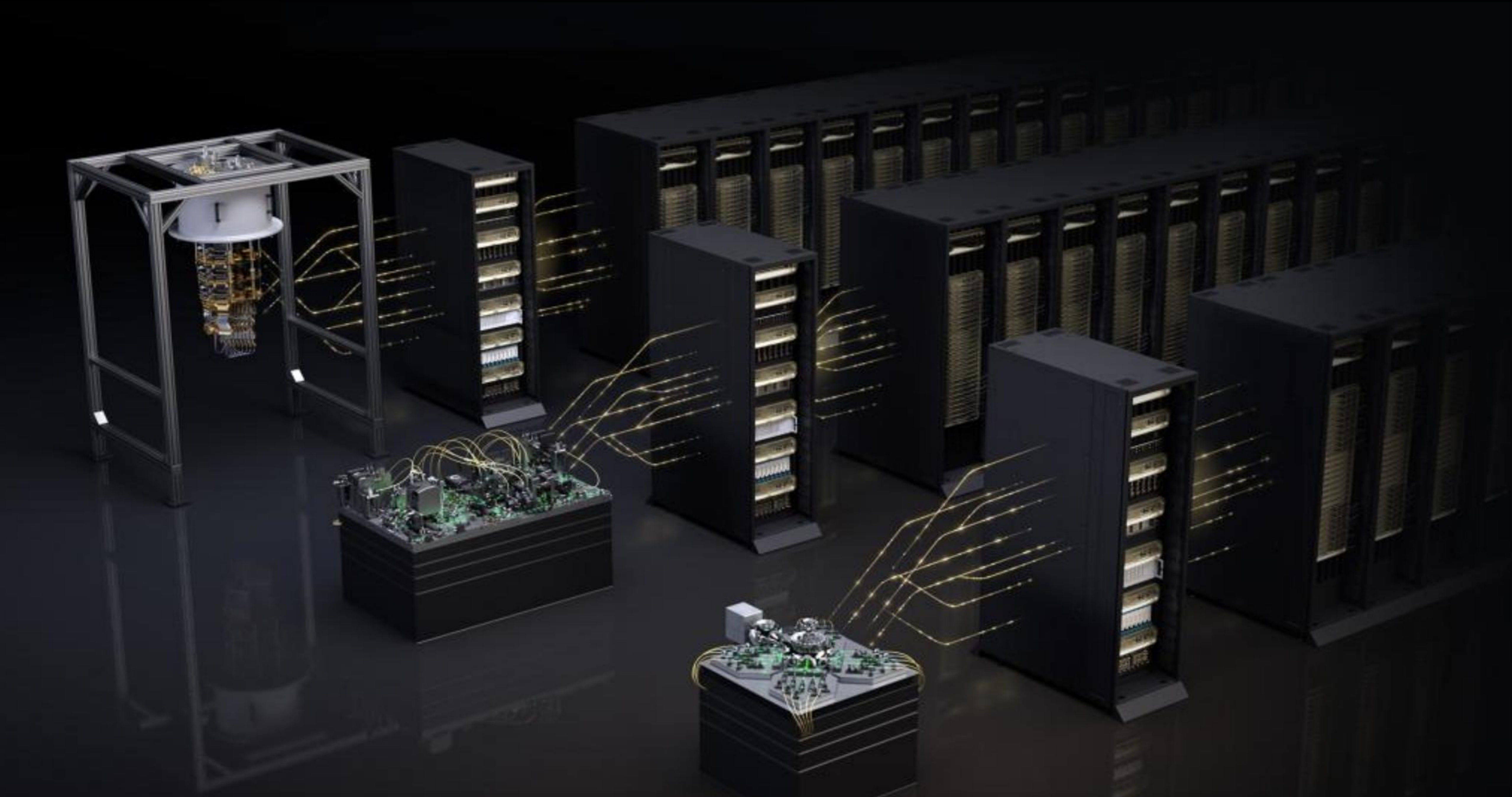
Stateless Hash-Based Digital Signature Standard

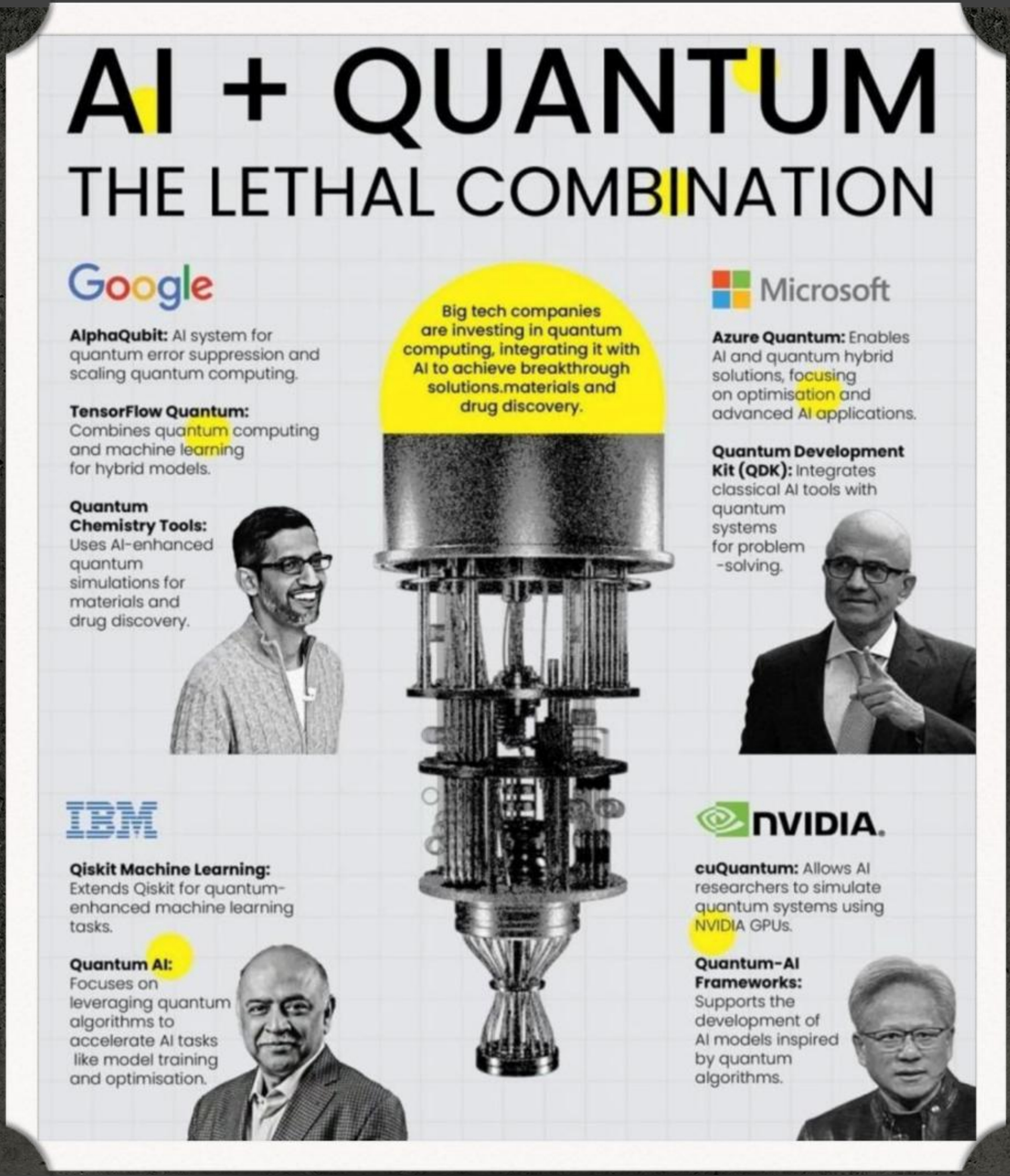
Category: Computer Security Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.205

Published: August 13, 2024





AI + QUANTUM

THE LETHAL COMBINATION

Big tech companies are investing in quantum computing, integrating it with AI to achieve breakthrough solutions.materials and drug discovery.

Google

AlphaQubit: AI system for quantum error suppression and scaling quantum computing.

TensorFlow Quantum: Combines quantum computing and machine learning for hybrid models.

Quantum Chemistry Tools: Uses AI-enhanced quantum simulations for materials and drug discovery.

Microsoft

Azure Quantum: Enables AI and quantum hybrid solutions, focusing on optimisation and advanced AI applications.

Quantum Development Kit (QDK): Integrates classical AI tools with quantum systems for problem -solving.

IBM

Qiskit Machine Learning: Extends Qiskit for quantum-enhanced machine learning tasks.

Quantum AI: Focuses on leveraging quantum algorithms to accelerate AI tasks like model training and optimisation.

NVIDIA.

cuQuantum: Allows AI researchers to simulate quantum systems using NVIDIA GPUs.

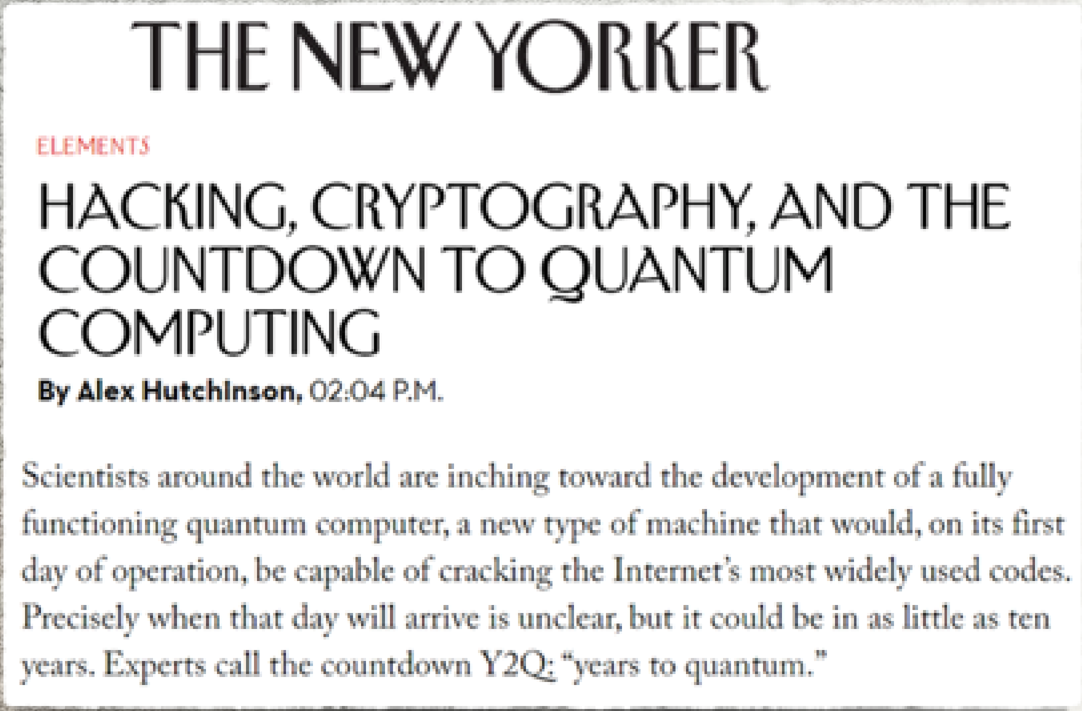
Quantum-AI Frameworks: Supports the development of AI models inspired by quantum algorithms.

IDQ
FROM VISION TO TECHNOLOGY
Quantum Random
Number Generator
Made in Switzerland
www.idquantique.com
US Patent No. 7,519,641
● PIN 1
Model n°: Quantis
Serial n°: 10EXPOA210

QUANTIS
QUANTUM RANDOM
NUMBER GENERATOR
IDQ
FROM VISION TO TECHNOLOGY
www.idquantique.com
MADE IN SWITZERLAND

Quantum Random
Number Generator

IDQ
SWISS
QUANTUM®



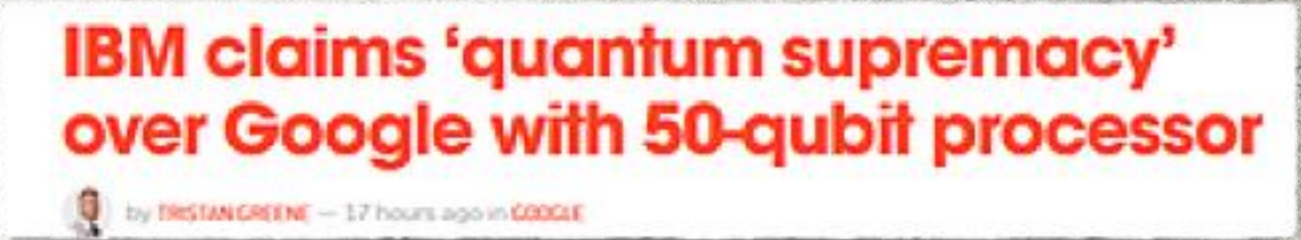
THE NEW YORKER

ELEMENTS

HACKING, CRYPTOGRAPHY, AND THE COUNTDOWN TO QUANTUM COMPUTING

By Alex Hutchinson, 02:04 P.M.

Scientists around the world are inching toward the development of a fully functioning quantum computer, a new type of machine that would, on its first day of operation, be capable of cracking the Internet's most widely used codes. Precisely when that day will arrive is unclear, but it could be in as little as ten years. Experts call the countdown Y2Q: "years to quantum."



IBM claims 'quantum supremacy' over Google with 50-qubit processor

by TRISTAN GREENE — 17 hours ago in GOOGLE

APIs / SDKs

Google

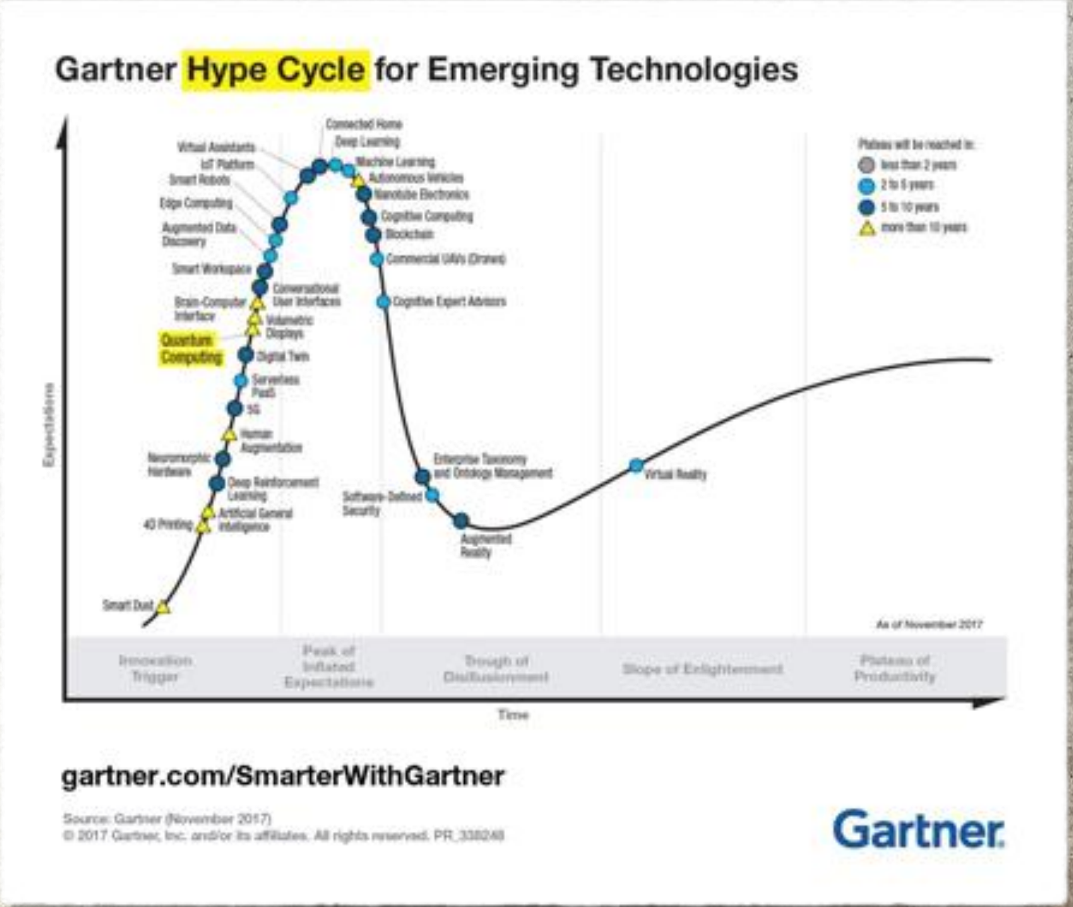
Quantum Computing Playground
http://www.quantumplayground.net/

IBM

Quantum Composer and QISKit software developer kit
https://quantumexperience.ng.bluemix.net

Microsoft

LIQUi|> is a software architecture and toolsuite for quantum computing
http://stationq.github.io/Liquid/



Gartner Hype Cycle for Emerging Technologies

gartner.com/SmarterWithGartner

Source: Gartner (November 2017)
© 2017 Gartner, Inc. and/or its affiliates. All rights reserved. PR_338248

Gartner.

NATIONAL LABORATORY FOR QUANTUM INFORMATION SCIENCES

The $10 billion National Laboratory for Quantum Information Sciences in Hefei will be the center of China's attempt to take the global lead in quantum computing and sensing.

CNTV

← Right Decision
Wrong Decision →

point of view.

Trust [trʌst] *n*

confidence in

dependence

tingent a

DANK JE

Quantum Computing: A New Beginning

Ramsés Gallego
CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT, Six Sigma Black Belt
Chief Technologist Cybersecurity, DXC Technology
ISACA Hall of Fame

Past International Vice President, ISACA, Board of Directors
President, ISACA Barcelona Chapter
Executive Vice President, Quantum World Association
Privacy by Design Ambassador, Government of Ontario, Canada
ramses.gallego@me.com @rams𝕏gallego

DXC TECHNOLOGY

ISACA®