De quantumcomputer en encryptie

MINISYMPOSIUM PARLEMENT & WETENSCHAP
TWEEDE KAMER
DEN HAAG, 10 MEI 2023

LIEVEN VANDERSYPEN

QuTech

QuTech is a collaboration between TU Delft TNO

Multiplying is easy, but how about factoring?

15 = 3 x 5

91 = . x . ?

437 = . x . ?

. . .

200 digits	1 day (impossible today)
201	2 days
202	4 days
203	8 days
210	1024 days ~ 3 years
220	3.000 years
230	3.000.000 years

Factoring takes *exponential* effort, i.e. is *intractable*!
Used in cryptography!

QuTech

The physics of computation

2500 BC

21st century

Classical bits (0 or 1)
Classical laws of physics

QuTech

Exponential power of quantum bits

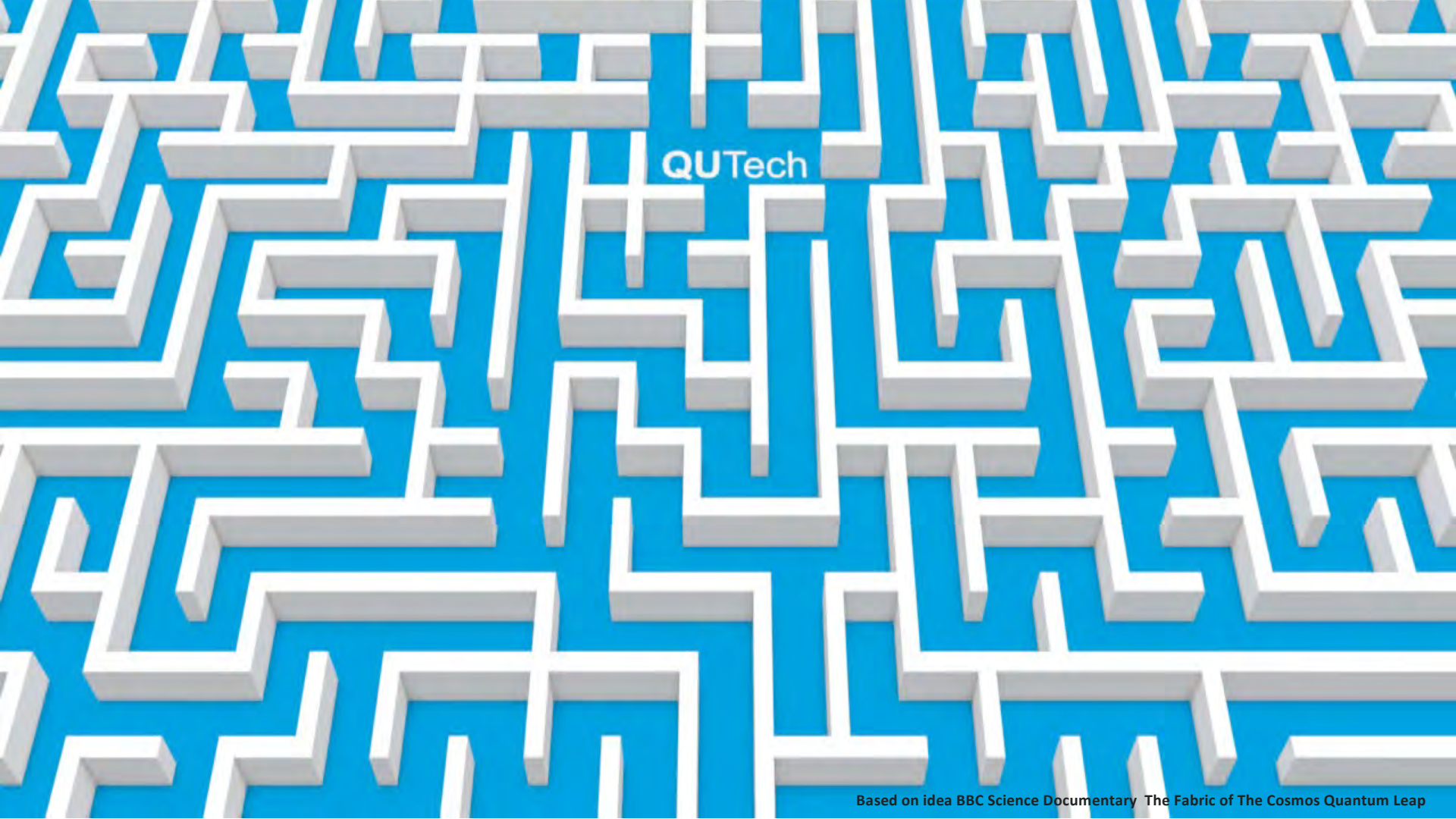
0 & 1

00 & 01 & 10 & 11

000 & 001 & 010 & 011 & 100 & 101 & 110 & 111

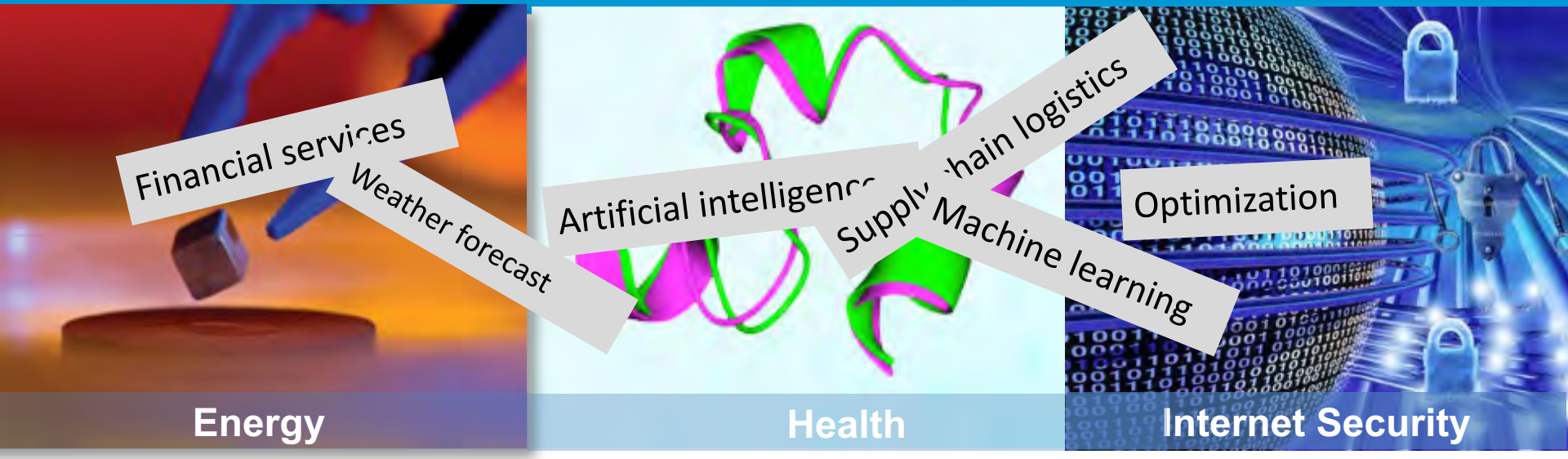
0000 & 0001 & 0010 & 0011 & 0100 & 0101 & 0110 & 0111 & 1000 & 1001 & 1010 & 1011 & 1100 & 1101 & 1110 & 1111

50 qubits (2^{50} ***complex*** amplitudes)
exceed memory of largest supercomputer



Based on idea BBC Science Documentary The Fabric of The Cosmos Quantum Leap

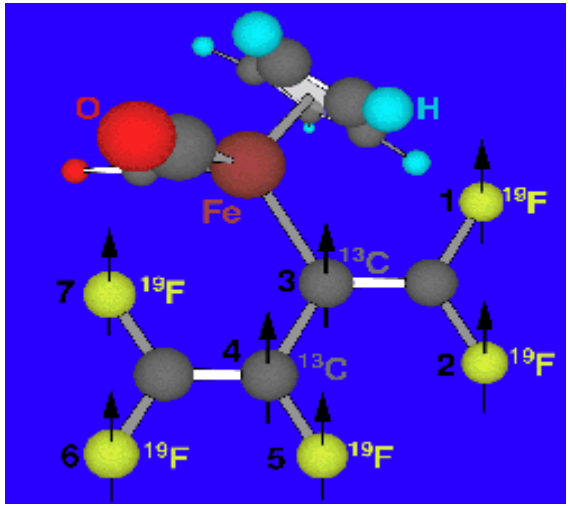
Specialized quantum algorithms can have broad application



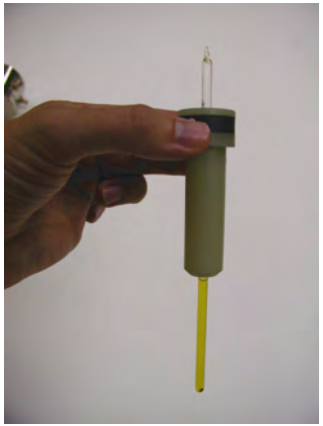
"The quantum computer may change our everyday lives in this century in the same radical way as the classical computer did in the last century." (Nobel citation 2012)

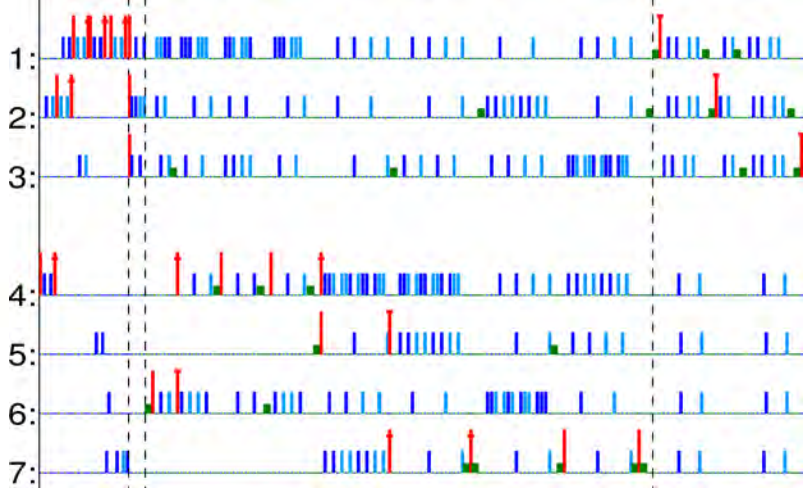
QuTech

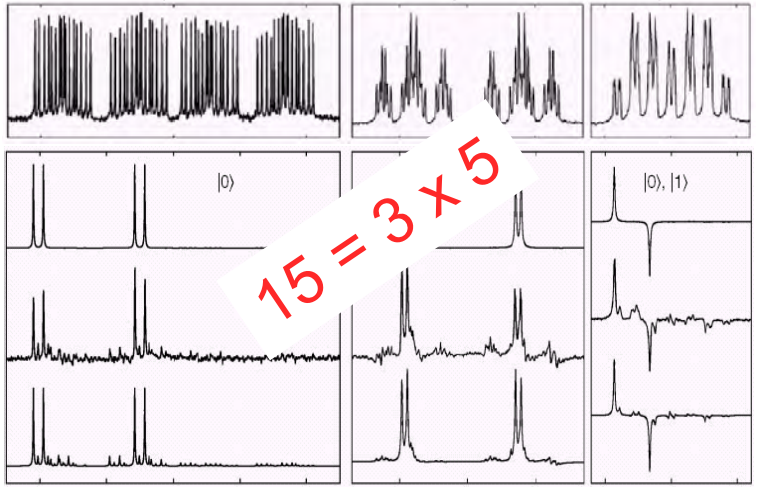
Early quantum factoring experiment



7 qubit molecule







QuTech

Vandersypen et al, Nature 2001

When will quantum computers outperform supercomputers?

When will they break encryption?

Article

Quantum supremacy using a programmable superconducting processor

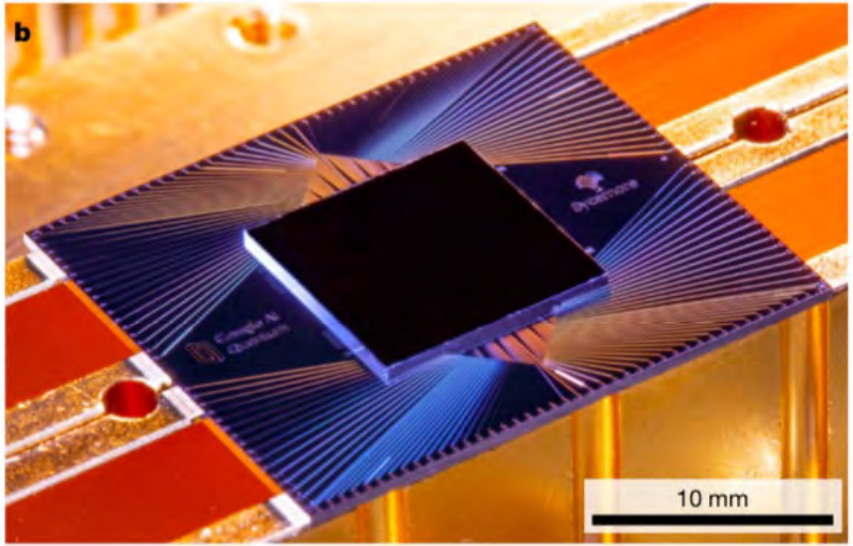
https://doi.org/10.1038/s41586-019-1666-5

Received: 22 July 2019

Accepted: 20 September 2019

Published online: 23 October 2019

Frank Arute[1], Kunal Arya[1], Ryan Babbush[1], Dave Bacon[1], Joseph C. Bardin[1,2], Rami Barends[1], Rupak Biswas[3], Sergio Boixo[1], Fernando G. S. L. Brandao[1,4], David A. Buell[1], Brian Burkett[1], Yu Chen[1], Zijun Chen[1], Ben Chiaro[5], Roberto Collins[1], William Courtney[1], Andrew Dunsworth[1], Edward Farhi[1], Brooks Foxen[1,5], Austin Fowler[1], Craig Gidney[1], Marissa Giustina[1], Rob Graff[1], Keith Guerin[1], Steve Habegger[1], Matthew P. Harrigan[1], Michael J. Hartmann[1,6], Alan Ho[1], Markus Hoffmann[1], Trent Huang[1], Travis S. Humble[7], Sergei V. Isakov[1], Evan Jeffrey[1], Zhang Jiang[1], Dvir Kafri[1], Kostyantyn Kechedzhi[1], Julian Kelly[1], Paul V. Klimov[1], Sergey Knysh[1], Alexander Korotkov[1,8], Fedor Kostritsa[1], David Landhuis[1], Mike Lindmark[1], Erik Lucero[1], Dmitry Lyakh[9], Salvatore Mandrà[3,10], Jarrod R. McClean[1], Matthew McEwen[5], Anthony Megrant[1], Xiao Mi[1], Kristel Michielsen[11,12], Masoud Mohseni[1], Josh Mutus[1], Ofer Naaman[1], Matthew Neeley[1], Charles Neill[1], Murphy Yuezhen Niu[1], Eric Ostby[1], Andre Petukhov[1], John C. Platt[1], Chris Quintana[1], Eleanor G. Rieffel[3], Pedram Roushan[1], Nicholas C. Rubin[1], Daniel Sank[1], Kevin J. Satzinger[1], Vadim Smelyanskiy[1], Kevin J. Sung[1,13], Matthew D. Trevithick[1], Amit Vainsencher[1], Benjamin Villalonga[1,14], Theodore White[1], Z. Jamie Yao[1], Ping Yeh[1], Adam Zalcman[1], Hartmut Neven[1] & John M. Martinis[1,5]*



My take (1):
An amazing technical achievement,
53 qubits under excellent control!

Article

Quantum supremacy using a programmable superconducting processor

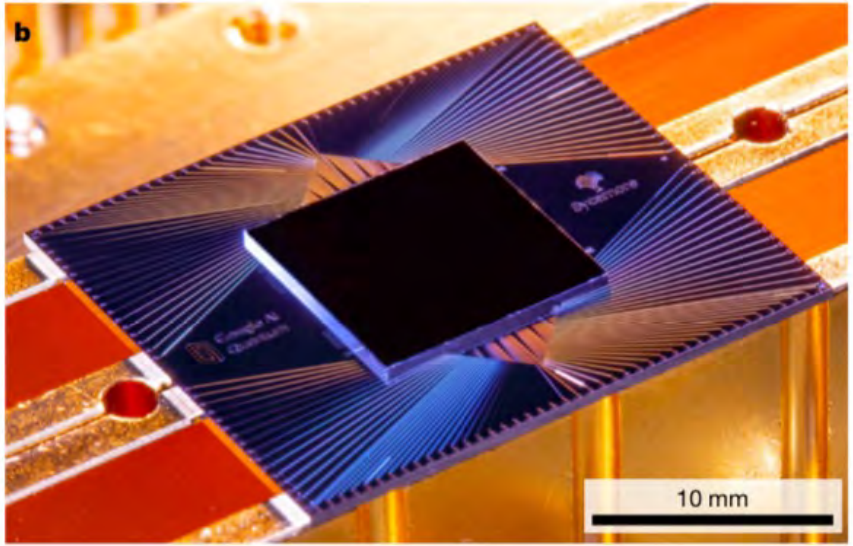
https://doi.org/10.1038/s41586-019-1666-5

Received: 22 July 2019

Accepted: 20 September 2019

Published online: 23 October 2019

Frank Arute[1], Kunal Arya[1], Ryan Babbush[1], Dave Bacon[1], Joseph C. Bardin[1,2], Rami Barends[1], Rupak Biswas[3], Sergio Boixo[1], Fernando G. S. L. Brandao[1,4], David A. Buell[1], Brian Burkett[1], Yu Chen[1], Zijun Chen[1], Ben Chiaro[5], Roberto Collins[1], William Courtney[1], Andrew Dunsworth[1], Edward Farhi[1], Brooks Foxen[1,5], Austin Fowler[1], Craig Gidney[1], Marissa Giustina[1], Rob Graff[1], Keith Guerin[1], Steve Habegger[1], Matthew P. Harrigan[1], Michael J. Hartmann[1,6], Alan Ho[1], Markus Hoffmann[1], Trent Huang[1], Travis S. Humble[7], Sergei V. Isakov[1], Evan Jeffrey[1], Zhang Jiang[1], Dvir Kafri[1], Kostyantyn Kechedzhi[1], Julian Kelly[1], Paul V. Klimov[1], Sergey Knysh[1], Alexander Korotkov[1,8], Fedor Kostritsa[1], David Landhuis[1], Mike Lindmark[1], Erik Lucero[1], Dmitry Lyakh[9], Salvatore Mandrà[3,10], Jarrod R. McClean[1], Matthew McEwen[5], Anthony Megrant[1], Xiao Mi[1], Kristel Michielsen[11,12], Masoud Mohseni[1], Josh Mutus[1], Ofer Naaman[1], Matthew Neeley[1], Charles Neill[1], Murphy Yuezhen Niu[1], Eric Ostby[1], Andre Petukhov[1], John C. Platt[1], Chris Quintana[1], Eleanor G. Rieffel[3], Pedram Roushan[1], Nicholas C. Rubin[1], Daniel Sank[1], Kevin J. Satzinger[1], Vadim Smelyanskiy[1], Kevin J. Sung[1,13], Matthew D. Trevithick[1], Amit Vainsencher[1], Benjamin Villalonga[1,14], Theodore White[1], Z. Jamie Yao[1], Ping Yeh[1], Adam Zalcman[1], Hartmut Neven[1] & John M. Martinis[1,5]*



My take (2):
A quantum processor that outperforms classical computers in computing
… *a random number*.

From quantum advantage to quantum practicality

Quantum advantage:
A programmable quantum device solves a problem that no classical computer can *feasibly* solve

John Preskill, arXiv:1203.5813, Arute et al, Nature 2019

Quantum practicality:
A programmable quantum device solves a *useful* problem that no classical computer can feasibly solve

James S. Clarke, https://newsroom.intel.com/editorials/what-it-will-take-make-quantum-computers-practical/#gs.j070ds

QuTech

Forbes

MONEY

Quantum Computing Is Coming, And It's Reinventing The Tech Industry

Q.ai - Powering a Personal Wealth Movement Contributor

Making wealth creation easy, accessible and transparent.

Follow

Jan 24, 2023, 09:30am EST

0

BASF Taps Quantum For Weather Forecasting

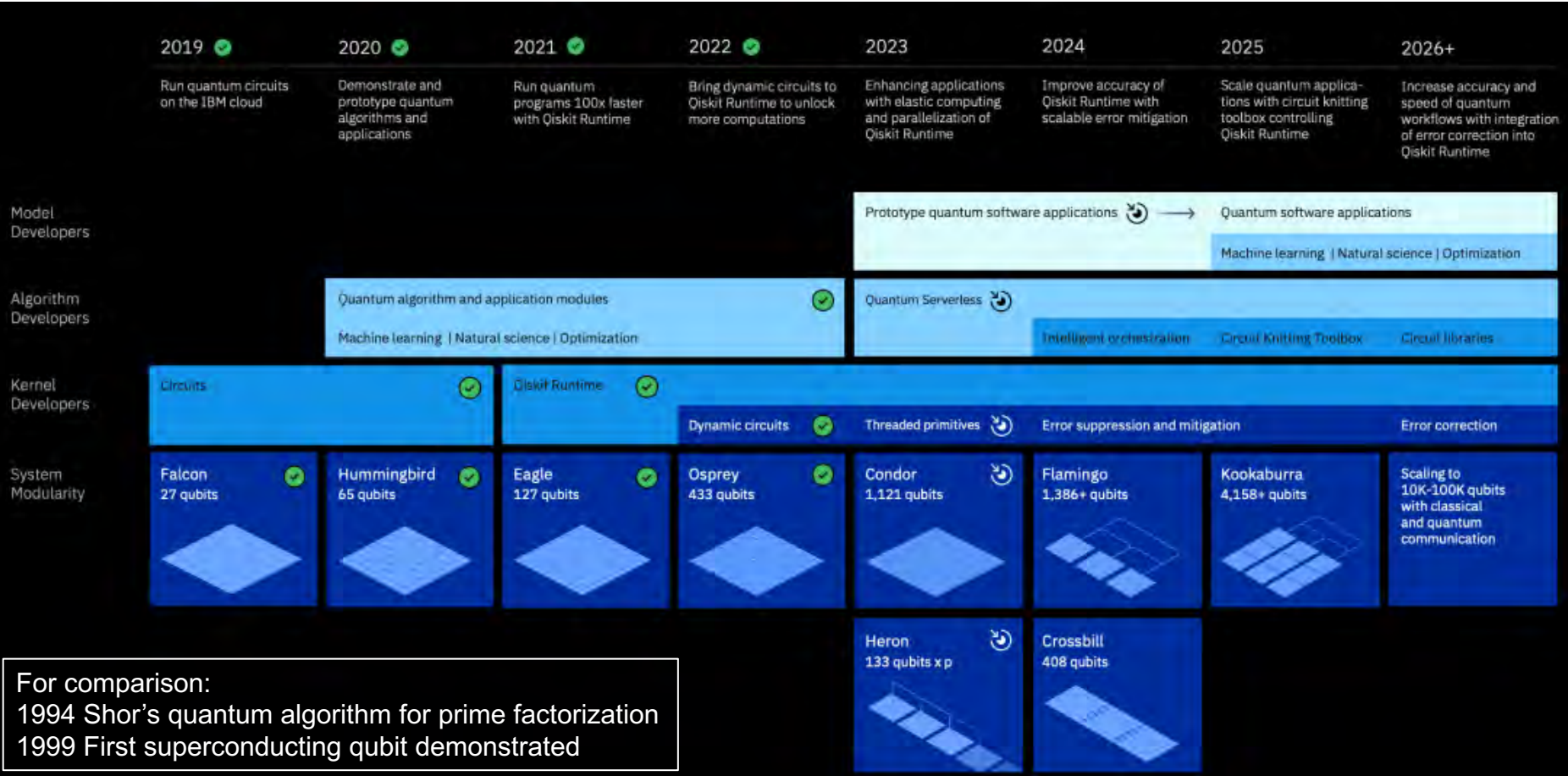
Digital agribusiness application aims to help maximize crop yield

Berenice Baker
July 21, 2022

2019-11-05

Quantum computers work in a completely different way from conventional computers. Volkswagen demonstrates the practical use of this technology for the first time with a pilot project for traffic optimization in Lisbon.

IBM Quantum Roadmap



For comparison:
1994 Shor's quantum algorithm for prime factorization
1999 First superconducting qubit demonstrated

What stands in between quantum advantage and practicality?

Errors inevitably accumulate due to “decoherence”

A *massive* redundancy is required to correct those errors
(suddenly millions of qubits are needed rather than a few thousand)

Extreme engineering effort

Breakthough ideas (in hardware or software)

Simple problems: possibly 5 years
Breaking encryption: > 10 years

QuTech

Closing remark: From quantum code breaking to quantum key distribution and networks

The laws of quantum physics guarantee that

no one can read, intercept, copy a quantum bit without getting noticed.

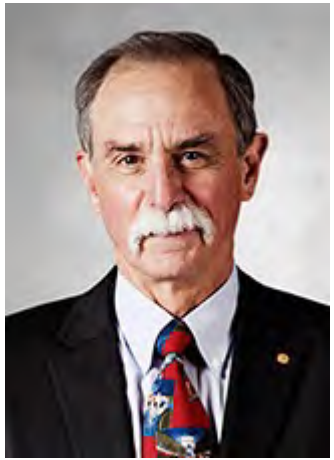
New path to encryption, not based on hard mathematical problems
but on laws of physics.

QuTech

Backup slides

What it takes: controlling individual quanta

Serge Haroche (ENS Paris)

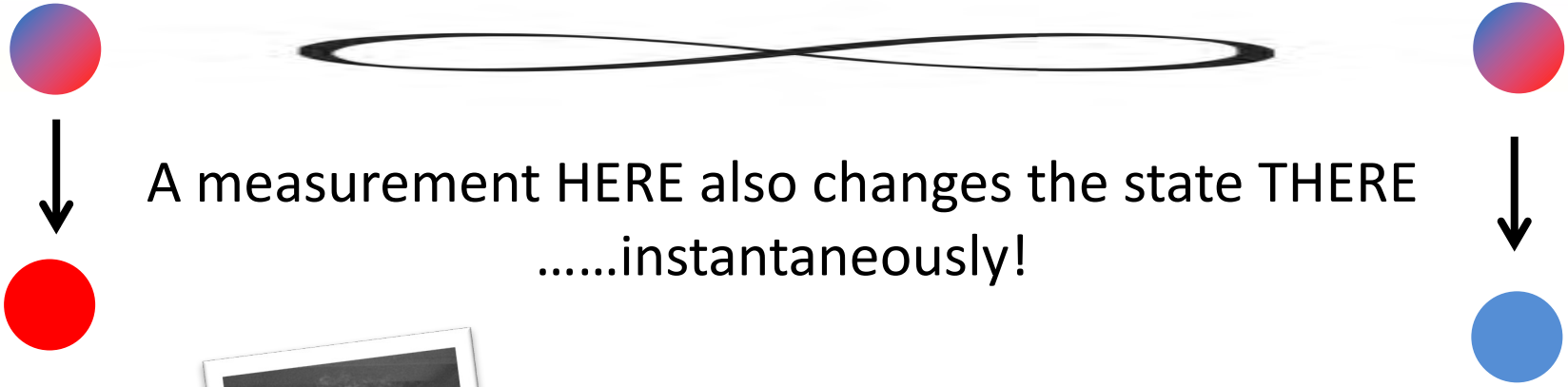


David Wineland (NIST)

Physics Nobel Prize 2012 *"for ground-breaking experimental methods that enable measuring and manipulation of individual quantum systems"*

… in a scalable way

Quantum entanglement



A measurement HERE also changes the state THERE
……instantaneously!

Einstein: "No spooky action at a distance!"

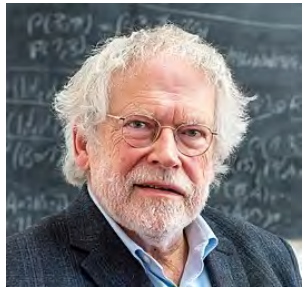
QuTech

It is how nature works!

Hensen et al., Nature 2015

A. Aspect (U Paris)

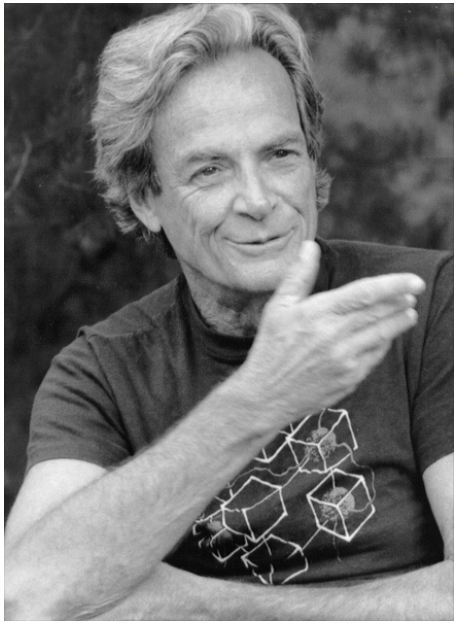
J. Clauser (USA)



A. Zeilinger (U Vienna)

QuTech

Beyond the surprise



Feynman: “Shut up and calculate!”

Quantum theory is useful!

Computing

Simulation

Communication

Sensing

. . .

QuTech