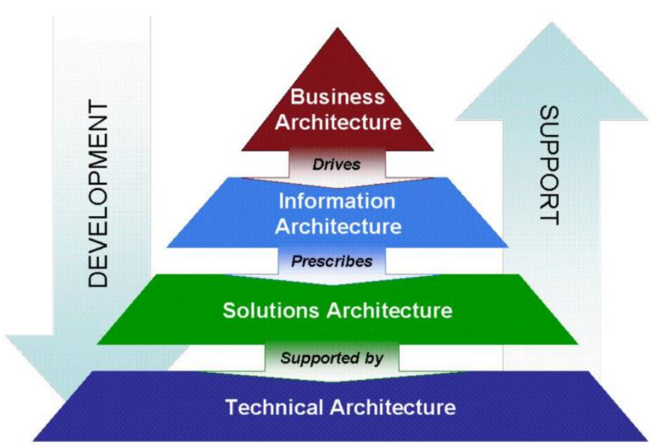
Virginia Information Technologies Agency

Enterprise Architecture Technical Brief

Quantum Computing

Robert Kowalke
January 2019



Summary

1. Quantum computing (QC) is as an emerging technology.
    a. Emerging technologies require additional evaluation in government and university settings.
    b. Emerging technologies may be used for evaluative or pilot testing deployments, or in a higher education research environment.
        i. The results of an evaluation or pilot test deployment of quantum computing should be submitted to the VITA Enterprise Architecture Division for consideration in the next review of the Enterprise Architecture for such technology.
    c. Any use, deployment or procurement of this technology beyond higher education research environments requires an approved Enterprise Architecture Change/Exception Request Form.

This technical brief defines the meaning of quantum computing and shows the impact quantum computing is anticipated to have on the commonwealth enterprise in the not too distant future.

Guidance from this technical brief is intended to help commonwealth agencies determine what they can do today to prepare for quantum technologies within their enterprises. This document also provides general VITA guidance for this moment in time with the current maturity of quantum computing.

For any comments, questions, and/or concerns with this technical brief, please contact VITA EA: ea@vita.virginia.gov

Contents

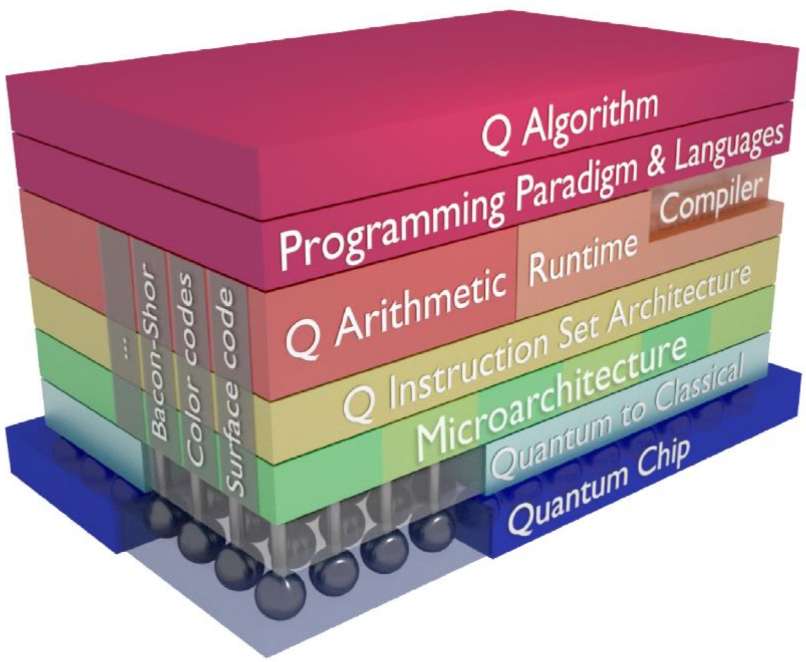


Figure 2.7: Quantum computer system stack [16]

VITA Quantum Computing (QC) Recommendations

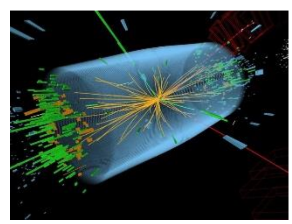
VITA recommends that:

- QC should not be ignored by agencies merely because it is an emerging technology.

- VITA assesses:

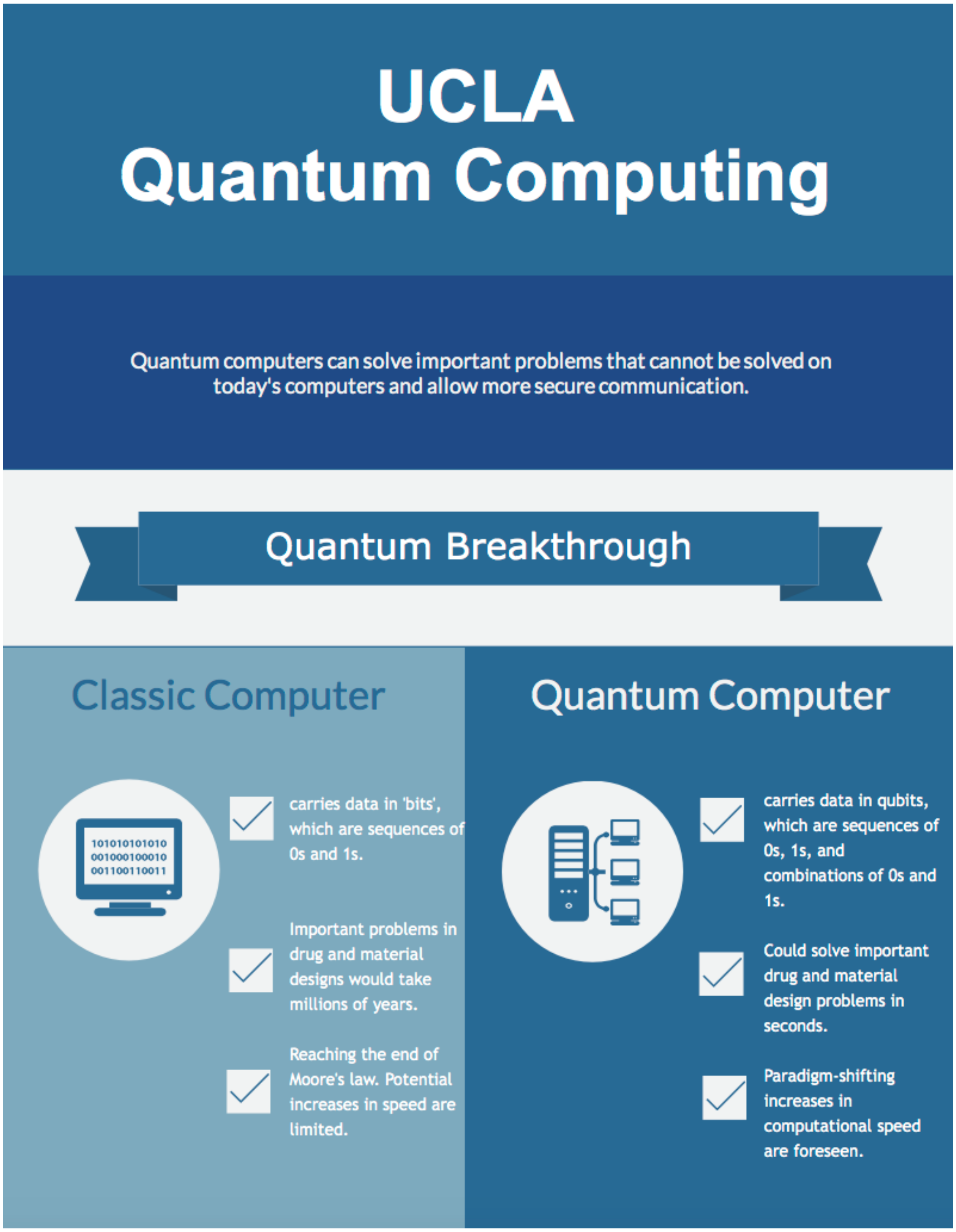
  - The voluntary catalyst for QC implementation within Virginia's executive branch will most likely be driven by financial use cases, given plans by the overall financial services industry for QC use around the year 2027 according to Gartner.
    - Moreover it could come through an area such as VDOT traffic optimization use cases given QC's excellence in solving such problems exponentially faster than classical computing.

  - The mandatory catalyst for QC implementation within Virginia's executive, legislative, and judicial branches will most likely be driven by QC's ability to breach and render obsolete many if not all current encryption algorithms.
    - It could also come through a quantum internet, which the European Journal of Physics considers the most promising application of emerging quantum technologies. [1]



- Agencies should identify and inventory dependency on quantum-vulnerable cryptographic algorithms, and prepare for their mitigation or replacement by creating an inventory of application dependencies.

[1] Towards a Quantum Internet by the European Journal of Physics on November 7, 2017. Obtained from the internet in December 2018.

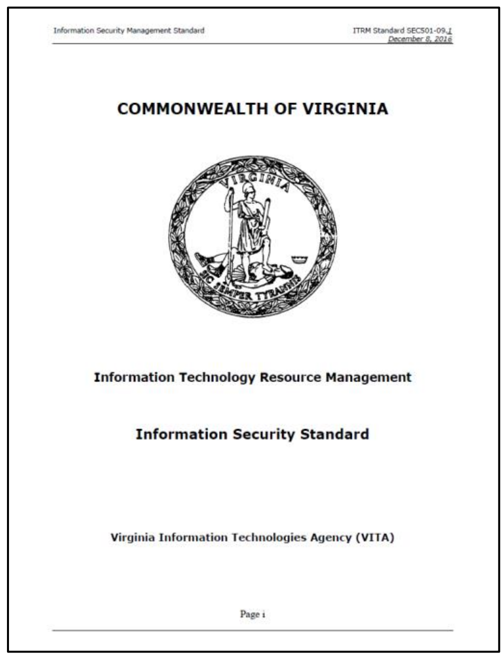

UCLA
Quantum Computing
Quantum computers can solve important problems that cannot be solved on today's computers and allow more secure communication.
Quantum Breakthrough
Classic Computer
101010101010
001000100010
001100110011
carries data in 'bits', which are sequences of 0s and 1s.
Important problems in drug and material designs would take millions of years.
Reaching the end of Moore's law. Potential increases in speed are limited.
Quantum Computer
carries data in qubits, which are sequences of 0s, 1s, and combinations of 0s and 1s.
Could solve important drug and material design problems in seconds.
Paradigm-shifting increases in computational speed are foreseen.

Supporting Quantum Computing Research

Commonwealth of Virginia – Information Security Standard – SEC501 [2]

Overview

- Quantum computing relates to SEC501's CA-7 – CONTINUOUS MONITORING section for emerging vulnerabilities in information technologies of which the ability for QC to break current encryption algorithms is a vulnerability requiring upcoming remediation.
- SEC501
    - Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: <snip>
        - (3) CONTINUOUS MONITORING | TREND ANALYSES <snip>
            - Supplemental Guidance: Trend analyses can include, for example, <snip> emerging vulnerabilities in information technologies <snip>.


Information Security Management Standard | ITRM Standard SEC501-09.1 December 8, 2016

COMMONWEALTH OF VIRGINIA

Information Technology Resource Management

Information Security Standard

Virginia Information Technologies Agency (VITA)

Page i

[2]Commonwealth of Virginia Information Security Standard – SEC501 by Virginia Information Technologies Agency (VITA).

What is Quantum Computing? [3]

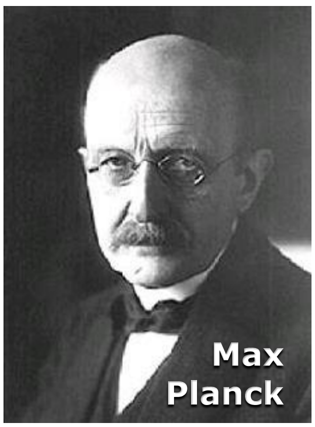
Overview

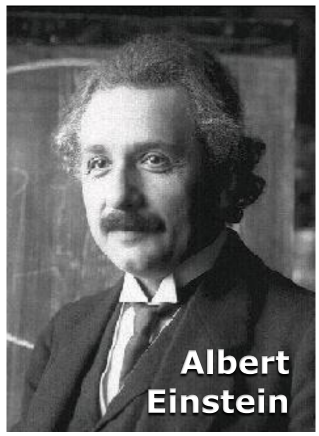
- Quantum computing is a field, which aims to build a computer based on the principles of quantum mechanics.

  - To explain quantum mechanics, suppose you throw a ball up into the air; the motion of the ball as it rises and falls is well-described by a set of mathematical laws known as Newton's laws, or classical mechanics.
    - Classical mechanics has been around for centuries, its foundations laid by the famous scientist Sir Isaac Newton.
  - Now, what happens if instead of throwing up a ball, you toss something much smaller - say, an electron or a photon?

[3] What is Quantum Computing by Quantum Computing Lab's Sevag Gharibian – 2018. Obtained from the web in December 2018.

- Just over a century ago, renowned physicists such as Max Planck, Albert Einstein, and Erwin Schrödinger were arriving at the startling conclusion that classical mechanics fails miserably in describing the behavior of such tiny subatomic particles.





- To address this, the physics community developed a new set of mathematical laws to describe this miniature world, known as quantum mechanics.

- The goal of quantum computing is to build a machine, which harnesses these new physical laws.

CIOs watch out: Here are seven (7) disruptions you might not see coming [4]

Overview

- The single largest challenge facing enterprises and technology providers today is digital disruption.
- There are several categories of disruption that organizations may not be prepared for and need to work to pre-empt, according to Gartner.

[4] CIOs watch out: Here are seven (7) disruptions you might not see coming by TechRepublic on October 18, 2018. Obtained from the web in December 2018.

- Quantum computing: Based on the quantum state of subatomic particles, quantum computing goes beyond the standard bits of traditional computing to offer high computational strength and parallelized computing.
- Advances in quantum computing could provide a stronger foundation for machine learning, artificial intelligence (AI), and data analytics.

University of Virginia's Pfister accomplishes breakthrough toward quantum computing [5]

Overview

- "Some mathematical problems, such as factoring integers and solving the Schrödinger equation to model quantum physical systems, can be extremely hard to solve," Pfister said.
    - "In some cases the difficulty is exponential, meaning that computation time doubles for every finite increase of the size of the integer, or of the system;" however, he said, this only holds for classical computing.
- Quantum computing was discovered to hold the revolutionary promise of exponentially speeding up such tasks, thereby making them easy computations.
    - "This would have tremendous societal implications, such as making current data encryption methods obsolete.
    - And it would also have major scientific implications, by dramatically opening up the possibilities of first-principle

[5] U.Va.'s Pfister accomplishes breakthrough toward quantum computing; article by the University of Virginia through the Science-X Network of Phys.org of July-15-2011. Obtained via the web in December 2018.

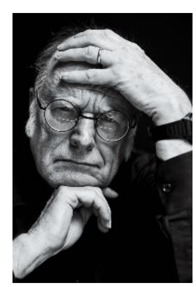
calculations to extremely complex systems such as biological molecules," Pfister said.

- "As far as we know, entanglement is actually the 'engine' of the exponential speed up in quantum computing."

Serious quantum computers are finally here. What are we going to do with them? [6]

Overview

- Google has been leading the charge toward quantum supremacy, while Intel and Microsoft also have significant quantum efforts.
  - And then there are well-funded startups including Rigetti Computing, IonQ, and Quantum Circuits.
  - No other contender can match IBM's pedigree in this area.
  - Quantum supremacy is where a quantum computer can solve problems a classical computer cannot.
- Charles Bennett of IBM Research (IBM since 1972) is one of the founding fathers of quantum information theory. His work at IBM helped create a theoretical foundation for quantum computing. Picture courtesy of Bartek Sadowski



[6] Serious quantum computers are finally here. What are we going to do with them? MIT Technology Review article in February 2018. Obtained from the web in December 2018.

- A picture of the IBM Q computer.

- The revolution will not really begin until a new generation of students and hackers can play with practical quantum machines.
- Quantum computers require not just different programming languages, but a fundamentally different way of thinking about what programming is.

D-Wave and Virginia Tech Join Forces to Advance Quantum Computing [7]

Overview

- D-Wave Systems Inc. and Virginia Tech have established a joint effort to provide greater access to quantum computers for researchers from the Intelligence Community and Department of Defense.

[7] D-Wave and Virginia Tech Join Forces to Advance Quantum Computing article by D-Wave News – Mar 13-2017. Obtained via the web in December 2018.

  - D-Wave and Virginia Tech will work towards the creation of a permanent quantum computing center to house a D-Wave system at the Hume Center for National Security and Technology.

D:Wave
The Quantum Computing Company™

- Under the agreement, D-Wave will work with Virginia Tech to enable their staff, faculty, and affiliates to build new applications and software tools for D-Wave quantum computers.
- Establishing a quantum computing center at the Hume Center will advance Virginia Tech’s mission of supporting national security, and providing access to technology that few researchers can leverage today,” said Mark Goodwin, deputy director and COO of the Hume Center.

Predicts 2018: Emerging Technologies Pave the Way for Business Reinvention [8]

Overview

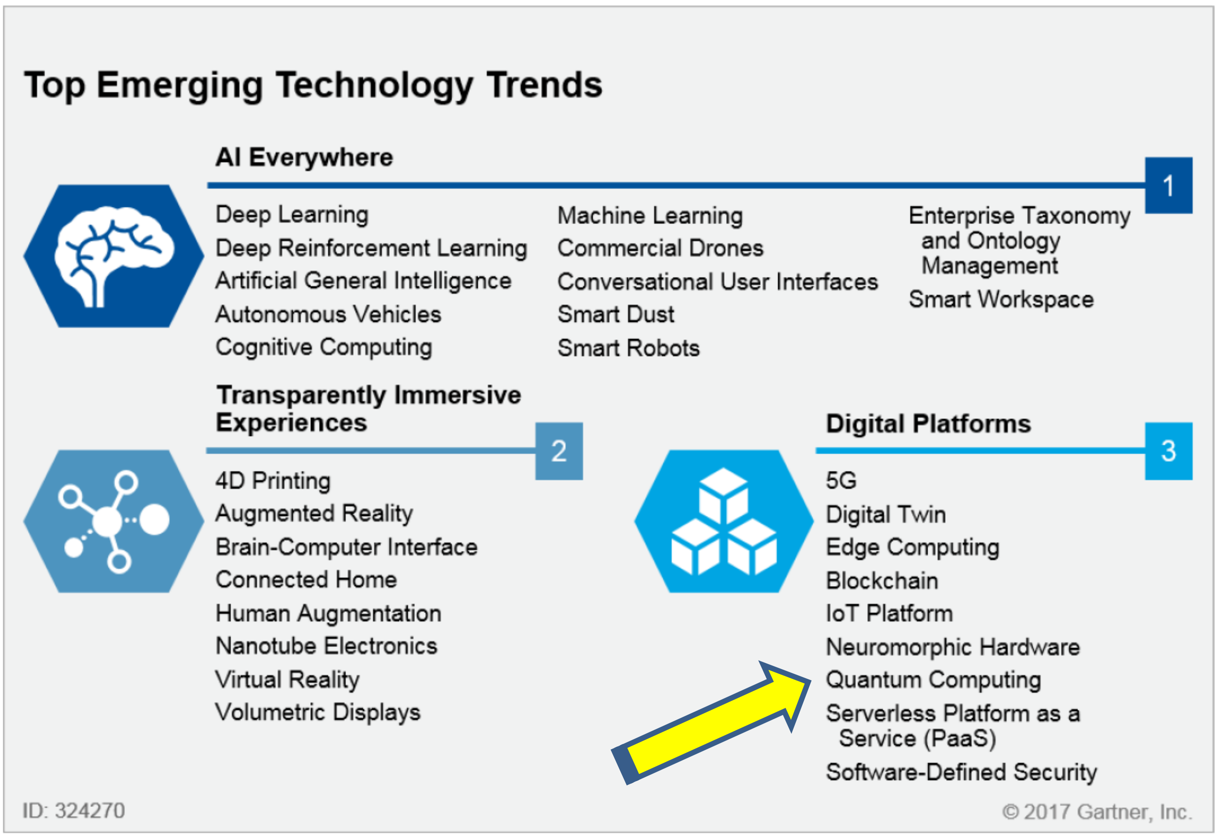
- By 2023, 20% of global enterprises will be budgeting for quantum computing (QC) projects, compared with less than 1% in 2017.
- QC is likely to take as long as a decade to reach broad mainstream adoption across industries.
- Cryptographic algorithms, such as RSA and Elliptic Curve, will be broken by QC, although existing key lengths are expected to remain safe for at least another five to seven years.

    - The National Institute of Standards and Technology (NIST) is hosting an open contest for selecting recommended Post Quantum Encryption algorithms and is expected to make a recommendation in a couple of years (the standard time frame for NIST algorithm selection).

[8] Predicts 2018: Emerging Technologies Pave the Way for Business Reinvention by Gartner. December 7, 2017.

- Inquiries about QC at Gartner have more than tripled every year for the past two years, with about 100 inquiries by October 2017, and is being driven by three factors:
    - Threat of QC to cryptography
    - Curiosity about the capabilities and time frames for specific applications
    - Potential use as a competitive advantage

Figure 1. The Top Emerging Technology Trends Driving Predictions



Source (December 2017)

- Some specific QC trends have emerged:
    - In financial services, organizations are looking at ways to get into the technology <u>as early as possible</u> because they want to develop a pool of programmers and application developers now,

so they do not have to search for them when there is more competition, and use them to develop early proofs of concept (POCs).

- QC development languages will be very different from existing ones, due to the different physics of QCs and a different mathematical basis.
  - There is a race to recruit developers now and build mind share for the products to become the standards as the hardware progresses.
- IBM has been offering Quantum Computing as a Service (QCaaS), and recently updated its computing capability from 17 to 50 qubits. Microsoft and Google have announced similar products.
- In healthcare, homomorphic encryption has emerged as a desired solution for privacy and for processing confidential data.
  - Homomorphism is a property of some forms of Quantum Resistant Encryption that allows computational operations (addition and multiplication) to take place on encrypted text, and the result of those operations appears in the decrypted text.
    - This supports the processing of cannot-be-read data, even when intercepted.
- Drug identification and molecular chemistry are using QC to model simple, but increasingly complex, molecules faster and more accurately than with classical techniques.
- In logistics, route optimization is a short-term goal that QC can begin to address, and is a problem QC is well positioned to solve.

        - Volkswagen AG, which is testing QC using GPS data from more than 10,000 taxis in Beijing, where they created an algorithm to calculate the fastest routes to the airport, while minimizing traffic. Traditional computer infrastructure required 45 minutes to complete that task; however, its quantum computer did it in a fraction of a second.
    - Cryptographic algorithms, such as RSA and Elliptic Curve, will be broken by QC, although existing key lengths are expected to remain safe for at least another five to seven years.
- The National Security Agency (NSA) issued an order that U.S. national-security employees and vendors must, "in the not-too-distant future," begin overhauling their encryption to guard against the threat posed by quantum computers.
    - Because national-security information must be protected for decades, the agency says new encryption needs to be in place before these machines arrive.
        - Otherwise, the NSA warns, code-breaking quantum computers would be "devastating" to national security.
    - NIST has begun looking for replacement algorithms for RSA and Elliptic Curve and has begun issuing new guidance for key and hash lengths.
    - QC will cause a re-evaluation of the security products that address encryption and hashing.

- It will drive significant changes, requiring evaluation of new products and vendors, and causing vendors to update their portfolios.

Higher Education’s Top 10 Strategic Technologies for 2017 [9]

Overview

STATE COUNCIL OF HIGHER EDUCATION FOR VIRGINIA

- Quite a few respondents indicated they were unfamiliar with particular technologies on the full list of 85 choices.
    - Some technologies are hardly surprising to find on this list, like quantum computing and in-memory computing.
- Quantum computing (20%) applies quantum mechanics to computation.
    - Vastly increases possible number of simultaneous calculations and enables tasks and computations that were previously out of reach.

[9] Higher Education’s Top 10 Strategic Technologies for 2017 by the Educause Center for Analysis and Research. Obtained via the web at https://er.educause.edu/~/media/files/library/2017/5/ers1707.pdf?la=en on December 3, 2018.

Application of Quantum Technologies for Practical Tasks [10]

Overview

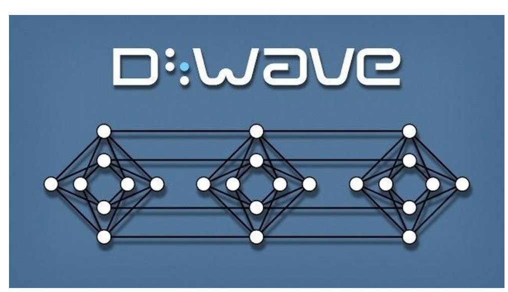
- Almost all large companies connected with information technologies are engaged in quantum computing – IBM, Google, and Microsoft carry out research in this area.

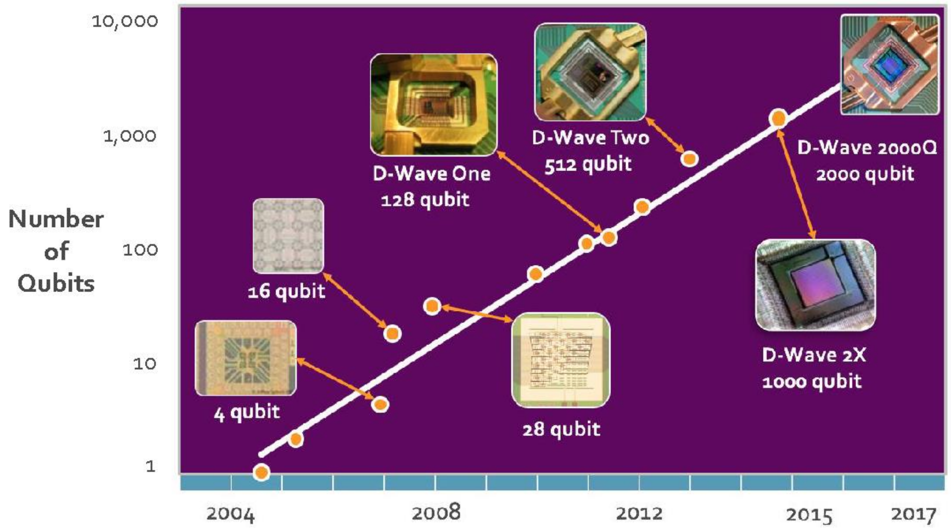
- The advantages of quantum computers are manifested in the following problems:
  - Rapid processing of huge databases
  - Optimizing processes, the nature of which is close to the task of the traveling salesman problem
  - Analyzing and processing scientific data with the identification of certain patterns
  - Decomposing numbers by prime factors using the Shore algorithm
- In the near future, the quantum Internet may become a separate branch of the conventional Internet.
  - Research groups around the world are developing chips to allow a quantum network connection for a typical computer, but so far it can only be used for certain tasks.
- Companies such as Google, IBM, and Microsoft propose using the resources of QC for various tasks, most of which are related to applied cryptography, e-commerce, and information protection.

[10] Application of Quantum Technologies for Practical Tasks, ISSA Journal of November 2017. Obtained via the web in December 2018.

- The challenge of quantum computing for classical cryptography is a real threat to many kinds of activity, including electronic commerce and electronic payments.
- With the help of quantum computers, one can optimize many processes from medicine to engineering.
- Application of quantum technologies in industry and communications:
    - The DWave 2000Q computer is a real quantum computer used for cybersecurity tasks.

- D-Wave is the world's first quantum computing company founded in 1999.
    - Public customers include Lockheed Martin, Los Alamos National Lab, Google, NASA Ames, Temporal Defense Systems.





- IBM Q.

- Google is showing new results in the development of quantum computers.

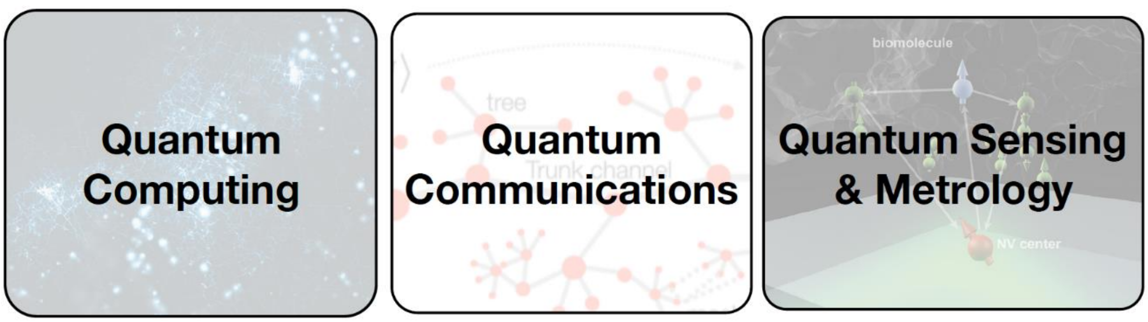
- Microsoft Station Q can be used for clarifying complex chemical processes with quantum computers.

- News about a project of scientists from Russia and the United States for creation of the first 51-qubit quantum computer testifies to the level of projects creating such devices.

Future Directions of Quantum Information Processing [11]

Overview

- The laws of quantum mechanics govern all physical systems at the most microscopic level.
- There are three subfields of quantum information processing:



- The greatest support for the fundamental science of quantum information processing has come from governments.
- The long term goal of quantum communication systems is a quantum internet – quantum computers connected via quantum communication channels.
- The participants were in unanimous agreement on their vision of the future of quantum information processing:
    - Quantum technologies will play a dominant role in the development of powerful computers, secure and high-rate

[11] Future Directions of Quantum Information Processing. A workshop on the emerging science and technology of quantum computation, communication, and measurement. Virginia Tech Applied Research Corporation (VT-ARC) – August 26, 2016. Obtained from the web in December 2018.

communication, and hyper-accurate sensors and imaging systems.

QUANTUM COMPUTING 5-YEAR OUTLOOK

Mid-scale quantum computers with 50–100 qubits capable of performing 10^4 quantum logic operations without quantum error correction.

High-fidelity logical qubits that function better than their physical constituents.

Fault-tolerant quantum logic operations on 1–2 logical qubits.

Special-purpose quantum information processors such as *quantum simulators* and quantum annealers with hundreds or thousands of qubits & applications to quantum chemistry or the demonstration of fundamental quantum effects such as entanglement over hundreds to thousands of qubits.

Quantum Random Access Memory (*qRAM*) prototypes.

Applications of 'mid-scale' quantum computers to quantum simulation, quantum machine learning, and demonstration of quantum supremacy.

Quantum Characterization, Verification, and Validation (qCVV) of mid-scale quantum circuits with quantum error correction.

QUANTUM COMPUTING 10-YEAR OUTLOOK

General-purpose quantum computers with 100-1000 qubits, with the ability to perform 10^5 quantum logical operations on multiple qubits with individual gate fidelities of 0.9999.

Fault-tolerant quantum logic operations on 10-100 logical qubits.

Special-purpose quantum computers such as quantum simulators and quantum annealers with hundreds or thousands of qubits & applications to quantum chemistry or the demonstration of fundamental quantum effects such as entanglement over hundreds to thousands of qubits.

Development of special-purpose deep quantum learning circuits.

Large-scale qRAM & quantum machine learning on medium-scale quantum computers.

Mid-scale, error corrected quantum computers.

Application of special-purpose quantum information processors to problems in elementary particle physics and quantum gravity.

QUANTUM COMPUTING 20-YEAR OUTLOOK

Large-scale universal, fault-tolerant quantum computers to factor, to solve hard linear algebra problems, to perform quantum simulation, and to perform machine learning. Such quantum computers will be able to perform a wide variety of computations that could not be performed classically.

Large-scale special purpose quantum simulators, annealers, integrated quantum optical circuits networked with general purpose quantum computers.

Quantum simulators established as a universal tool for the characterization of fundamental quantum effects and the design of novel quantum technologies and materials.

Strong experimental and theory connections between quantum information science and other fields, such as high energy physics, quantum gravity, chemistry, and computational biology.

- Achieving the full potential of quantum information processing would result in:
  - unhackable computer systems
  - quantum machine learning techniques that can find patterns that are inaccessible to any classical learning method
  - GPS that determines position at the submillimeter scale
  - inertial guidance and navigation systems that maintain the precision of GPS over weeks
  - detection and imaging systems that surpass the Rayleigh diffraction limit by orders of magnitude.

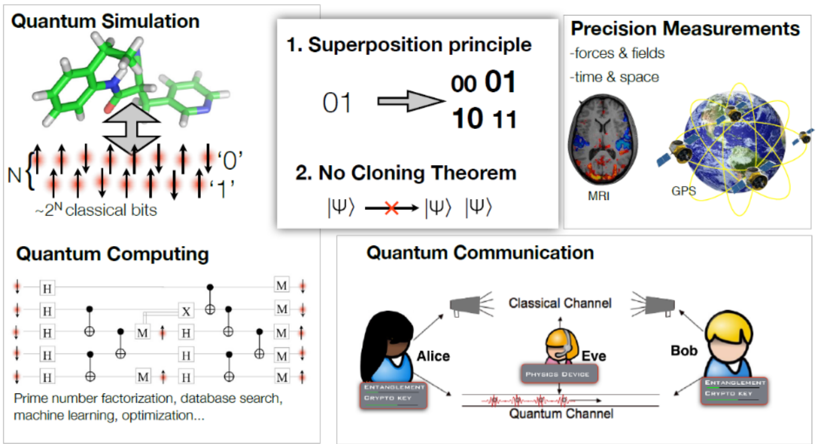


Figure 2. Three key areas of quantum technologies: Quantum Simulation and Computing; Precision Measurements and Metrology; and Quantum Communications. These technologies are enabled by the laws of quantum mechanics. Two essential underlying principles are the superposition principle (quantum states can be in multiple distinct observables states simultaneously, even when these states are delocalized) and the no-cloning theorem (quantum mechanics doesn't allow an unknown state to be copied).

- A mid-scale quantum computer with fifty qubits, capable of performing thousands of coherent operations, crosses an important threshold, for it is at this scale that it becomes effectively impossible to characterize and simulate the behavior of such a quantum computer using even the most powerful classical computers.
    - A quantum computer with fifty qubits requires 250 ≈1015 memory sites on a classical computer merely to record the state of the quantum device!
    - To simulate the dynamics of a mid-scale quantum computer on a classical computer requires the ability to exponentiate 1015 by 1015 matrices.
        - These requirements will lie outside of the capability of classical computers for many years to come.
    - Simulating quantum computers with one hundred qubits, which is a reasonable 5-10 year goal to develop would require classical computers with around 1030 memory sites and capable of exponentiating 1030 by 1030 matrices, which is unlikely to happen for decades, if ever.
- Quantum computers are right now on the verge of breaking the barrier of classical computation.

- We are now poised for the development of a quantum internet to exchange quantum information and distribute entanglement among quantum computers.
  - A quantum internet has new capabilities that would be impossible in a classical world, including:
    - long-distance unconditionally-secure communication
    - precision sensing and navigation
    - distributed quantum information processing
  - Some essential components of the quantum internet have already been deployed, including:
    - quantum key distribution links over fiber, free-space, and initial satellite links
    - quantum teleportation in deployed fiber
    - the first optical links between entangled NV spin systems

QUANTUM COMMUNICATION 5-YEAR OUTLOOK	QUANTUM COMMUNICATION 10-YEAR OUTLOOK	QUANTUM COMMUNICATION 20-YEAR OUTLOOK
Efficient on-demand sources of entangled photon pairs or larger entangled photonic micro-clusters; investigation of new photon source concepts to close the gap between system-level requirements on photon efficiency and experimental capability.	Advanced photonic components and protocols for quantum key distribution at rates hundreds of Mbit/sec over metro-scale (~50km) distances in network topologies that are upgradable with quantum repeaters.	Networks capable of distributing entanglement at high rates over continental length scales, including efficient coherent interfaces to various types of quantum computers (atoms, solid-state, microwave...).
Optical communication systems operating near the quantum limit, for example using chip-based multi-mode optimal receivers to approach channel capacity limits.	Development of on-demand single and entangled photon pair sources with sufficient purity, efficiency, and indistinguishability to produce large photonic cluster states.	Quantum networks for efficient links between many quantum memories, high-speed quantum teleportation, cryptography, and modular quantum computing.
Single photon detectors with >0.99 detection efficiency.	The development of photon-loss-protected photonic states for forward error correction, allowing new forms of long-range quantum state transfer, cryptography, and mid-scale photonic quantum information processors.	Small quantum networks are connected into global "quantum internet" whose functions, beyond secure communication and parallel computing, will include many other applications, including quantum digital signatures, quantum voting and secret sharing, anonymous transmission of classical information, and a host of sensing and metrology applications.
Quantum cryptography with secure bit transmission rates of more than 10^8 per second.	Quantum repeater links beating repeaterless quantum cryptography rate-loss bounds	
Efficient quantum interfaces between long-lived stationary memories (atomic and solid-state) and photons.	The demonstration of long-distance quantum communication channels consisting of multiple quantum repeaters, beating repeaterless quantum cryptography bounds.	
Prototype quantum repeaters and linking of two or more small-scale quantum computers via high-fidelity quantum communication channels.	High bit rate quantum cryptography over 1000s of kilometers. Construction of prototype quantum internet consisting of multiple medium scale quantum computers connected via high fidelity quantum communication channels.	
Efficient quantum frequency conversion between telecom photons and atom-like memories as well as superconducting microwave cavities.		

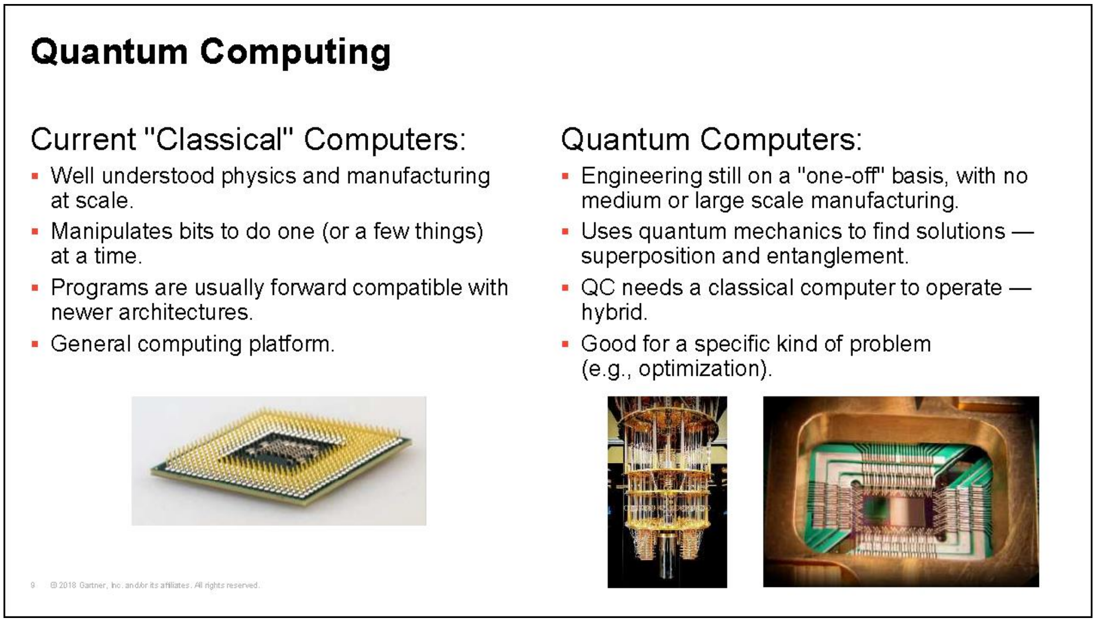
The "In Your Face" Disruption Few Understand and Some Fear [12]

Overview

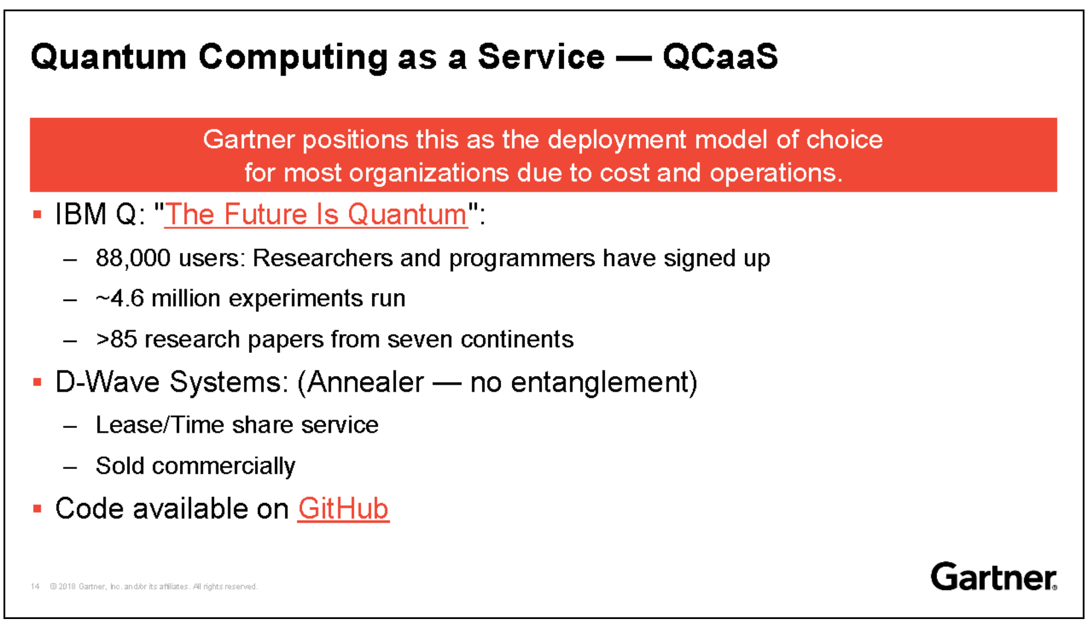
Research and presentation by Mr. Matthew Brisse of Gartner at the Gartner Catalyst 2018 Conference.

- Quantum computing (QC) will totally change the computing science landscape in higher education.
- By 2023, 20% of organizations will be budgeting for QC projects compared to less than 1% today.
- Without hype, there is no funding.
- There are 62 QC companies currently.
- QC is not ready for mainstream today.
- QC is non-deterministic.
  - For example: 1+1 = 99.99% probability the solution is 2.
- Commercially viable for specific problems in six to ten years.
- Machine learning is the biggest quantum use case.
- Financials services planning on QC usage in 2027.

[12] Gartner Catalyst Conference 2018. Obtained via Gartner and various research in October 2018.

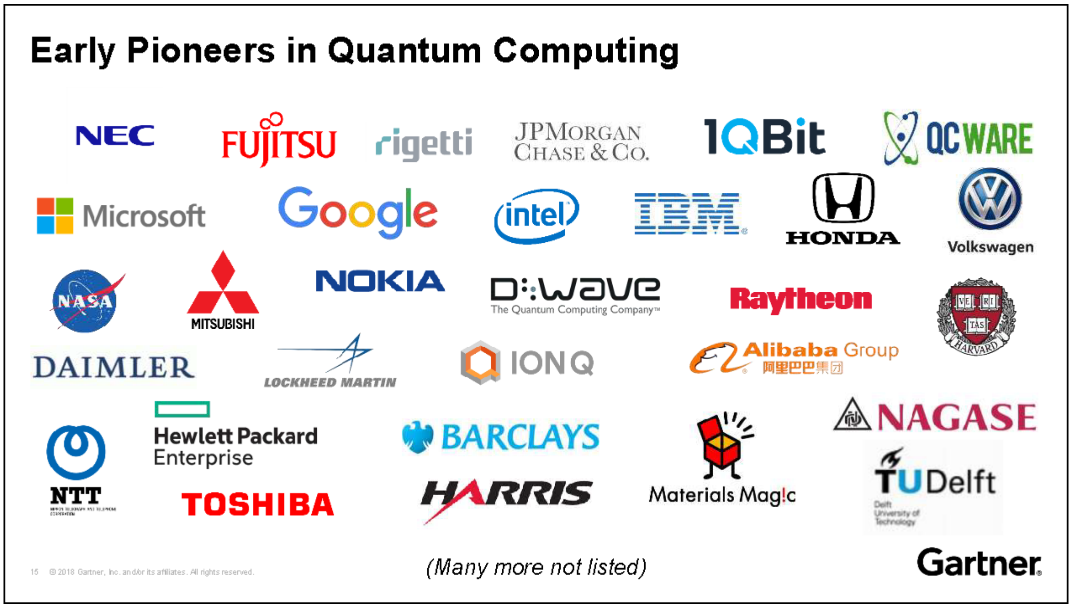


- 4IR = Fourth Industrial Revolution – Quantum, Artificial Intelligence (AI), Machine Learning, etc.

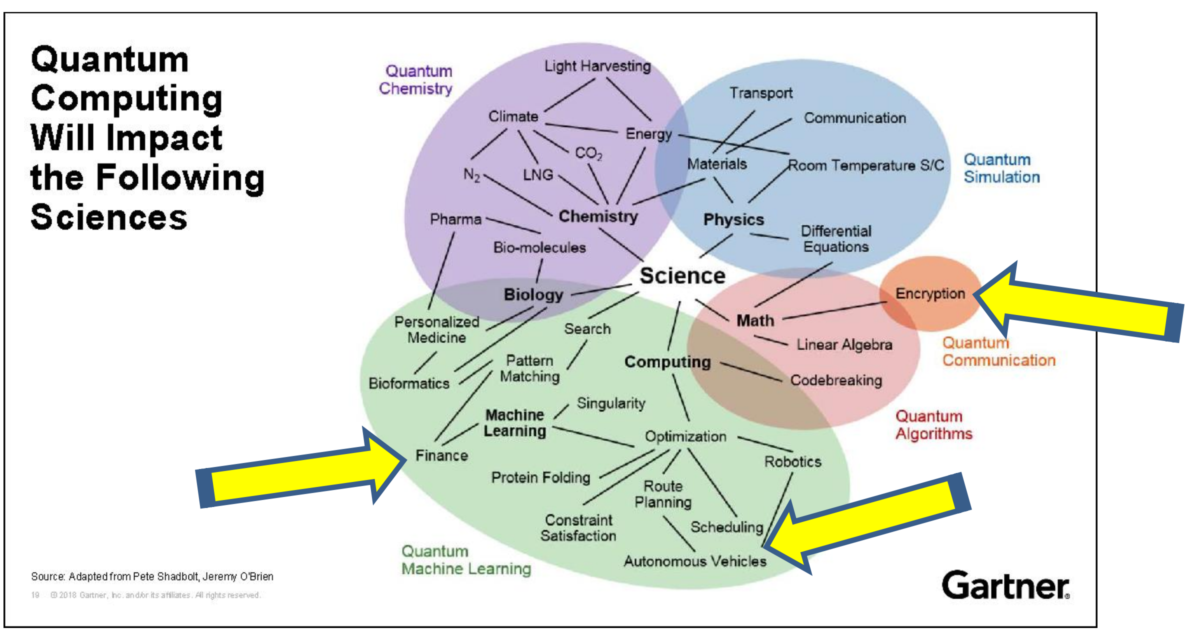


- Gartner has received over 300 calls from CIO's / CTO's on Quantum through July 2018.
- Quantum algorithms are coming first for use in machine learning.

•



- All quantum chips are one off's.
- Exponential speed up – N^{300} instead of N^2 (1's and 0's).
- Computational scientist will take problems to quantum system for highest probability solutions.



Quantum Impact on Security — What Is Vulnerable?

Cryptographic Algorithm	Type	Purpose	Impact When Large-Scale Quantum Computers Are Achieved
AES-256	Symmetric key	Encryption	Probably okay
3DES	Symmetric key	Encryption	Must be deprecated
SHA-2, SHA-3		Hashing	Quantum safe algorithms
FIPS PUB 186-4	Digital signature standard	Signatures (public key + hashing)	No longer secure
SP 800-56A/B	Pairwise key establishment schemes	Key establishment	No longer secure
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key establishment	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key establishment	No longer secure

Source: NIST Guidance

Gartner

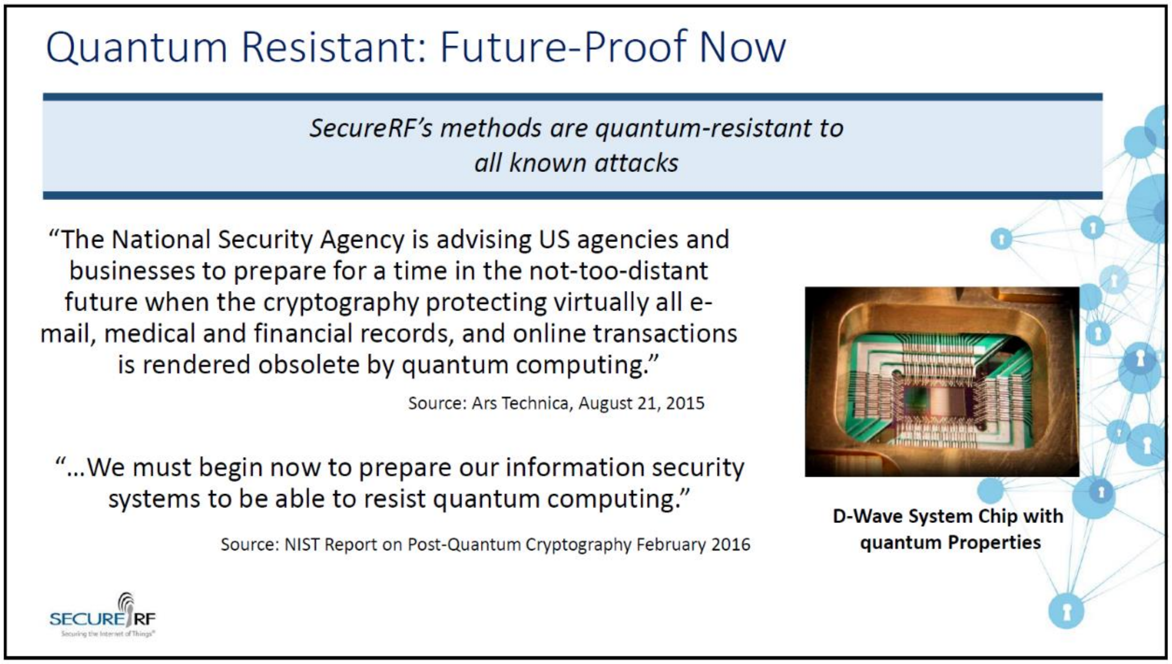
Prepare for Post Quantum — What Is Vulnerable?

Technology	Application	Impact
Public Key Infrastructure (PKI)	Certificates Key management	PKI will need to be moved to quantum-safe cryptography Existing PKI will be deprecated Credentials will need to be reissued
Digital Signatures	Contracts (mortgages, agreements) that extend beyond 2022 Secure email Timestamps Hashed-linked logs and records	PKI-dependent Hash values will need to be lengthened
Cryptographic Hash Functions	Integrity checks Logs Password security	Hash values will need to be lengthened
Blockchain/ Public Ledgers	Contracts Cryptocurrency Proof of work	PKI-dependent Credentials will need to be reissued Hashes lengthened Blockchains may need to be resigned
Data Security	Stored/Encrypted data SSL/TLS	Personal records where data needs to be secret for decades 70 years or more PKI-dependent Key storage and exchange will need new protocols

Move to quantum safe algorithms as providers make them available ...

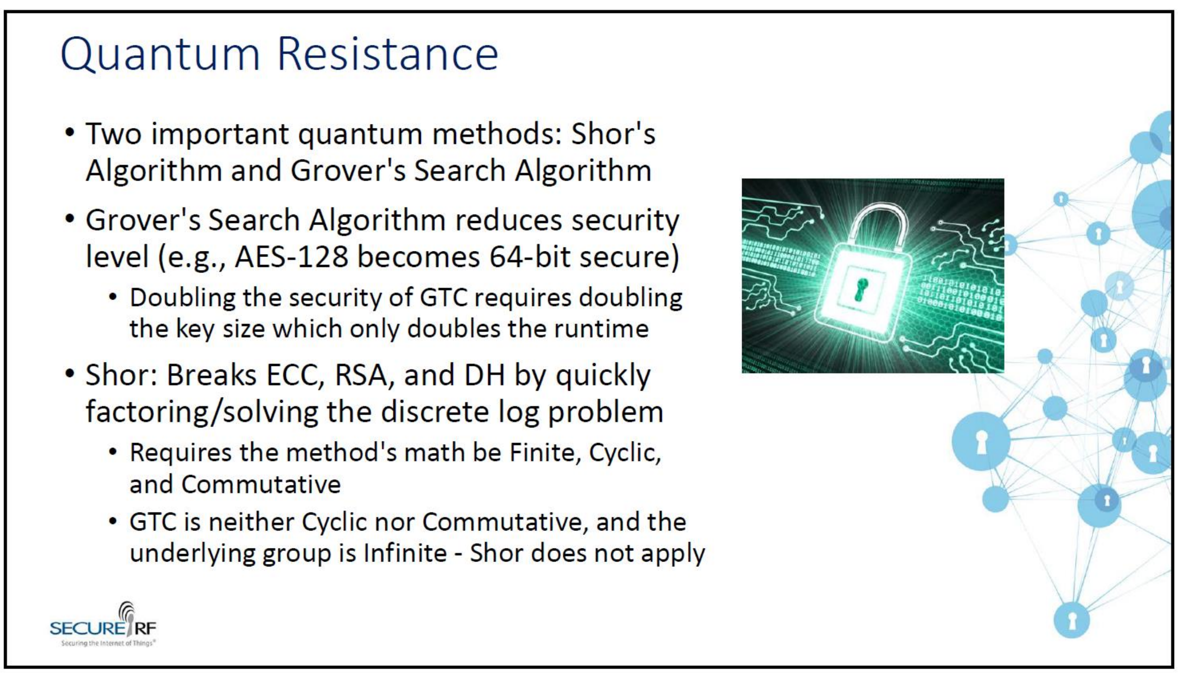
Source: NIST Guidance

Gartner



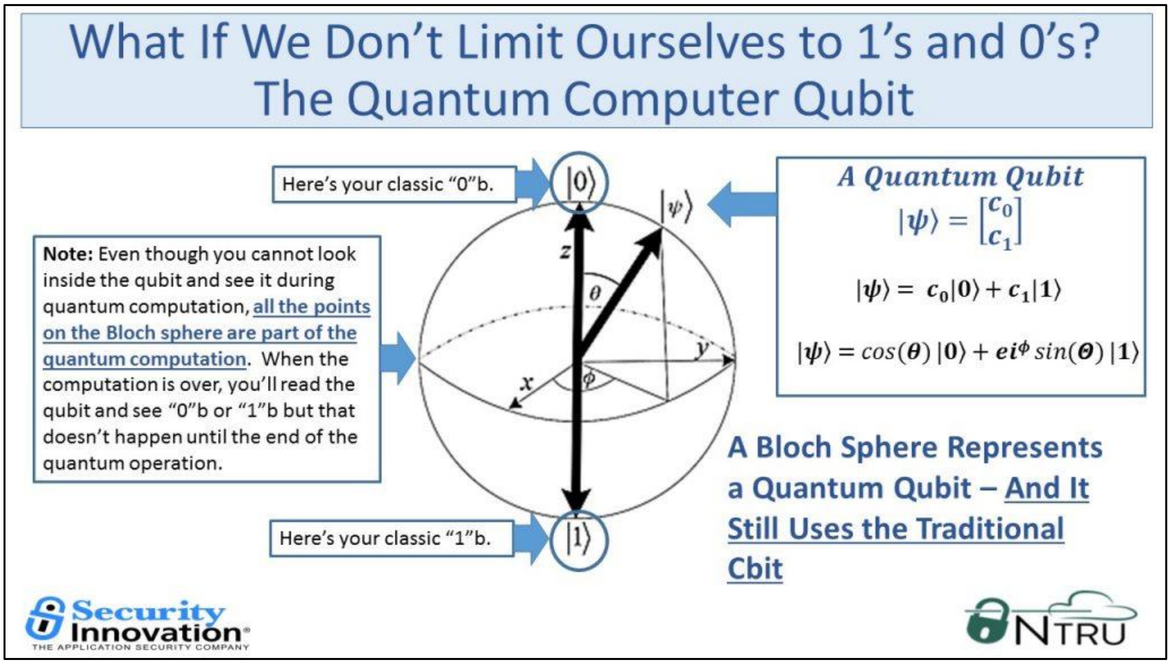
Security Essentials for IoT Product Developers – SecureRF 2017

- You will not be using a Quantum computer to run your Microsoft Word app.
- Banks have to be concerned about quantum.



Security Essentials for IoT Product Developers – SecureRF 2017

- Quantum computing positions the qubits and then reads them.
- Qubit = electrons.
- Need 150-300 qubits to do meaningful work.
- Need an oscilloscope to read qubits.



- To be considered quantum a machine must do entanglement.
  - D-Wave is technically not quantum because it can't do entanglement.
- Free quantum computing is available on the web today.
- Quantum computers currently must be tuned twice a day.
- Do not ignore quantum computing!

Quantum Cloud Services (QCS) is entering arena with big prize offer [13]

Overview

- MIT Technology Review identified what sets quantum computing apart from traditional computing:
  - Traditional machines use standard digital bits that can represent either 1 or 0, but qubits can be both at the same time.
  - "Adding just a few extra qubits to a machine – and linking them via a phenomenon known as 'entanglement' – creates exponential leaps in computing power."
- QCS tackles the problem with a data center containing both quantum computers and classical computers in a system optimized to run entire hybrid algorithms.
- Rigetti Computing will be granting early access to Quantum Cloud Services in the coming weeks (September 2018).
- Sign up to reserve a QMI today at rigetti.com.

Roland Berger Trend Compendium 2030 [14]

Overview

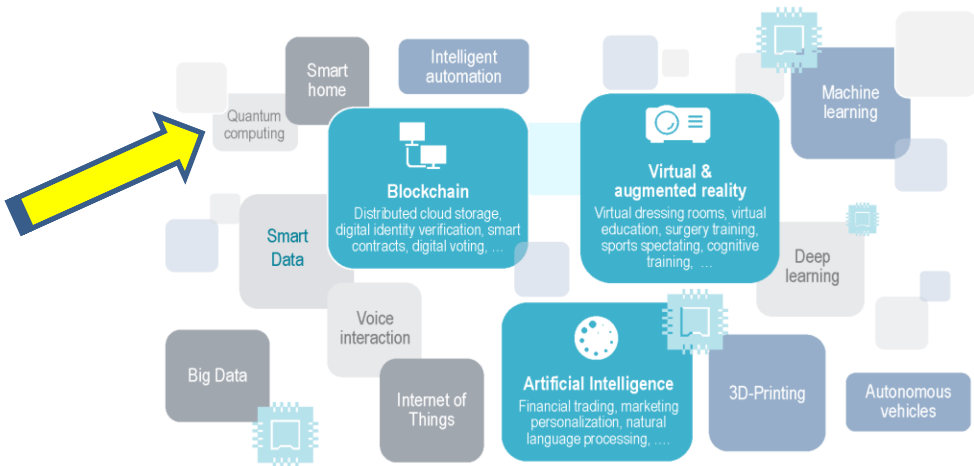
- A global trend study compiled by the Roland Berger Institute (RBI) describing the most important megatrends that will shape the world between now and 2030.

[13] Quantum Cloud Services is entering arena with big prize offer by Tech Xplore on September 10, 2018. Obtained via the web in December 2018.
[14] Roland Berger Trend Compendium 2030 in October 2017; Megatrend 5 – Dynamic Technology and Innovation, Roland Berger Institute. Obtained via the web in December 2018.

- These megatrends will have a broad impact on the environment of companies, strongly influencing challenges and opportunities of their business
    - Megatrend 5 – Dynamic Technology and Innovation.

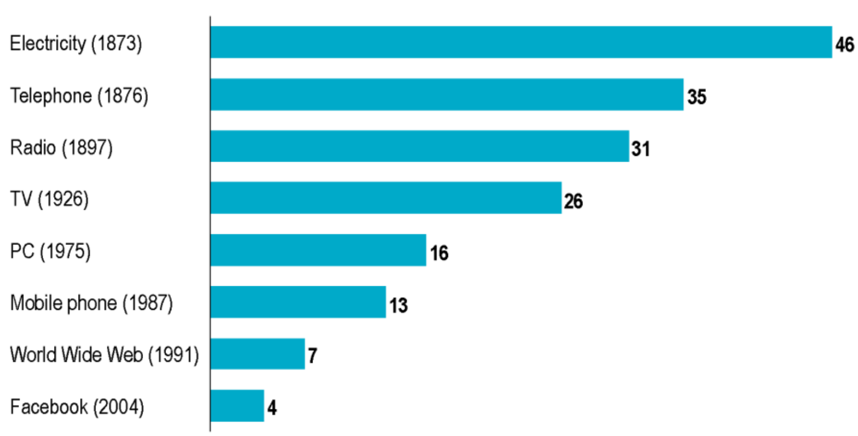
New technologies emerge that strongly impact our daily life and the way we do business

Overview of technology trends



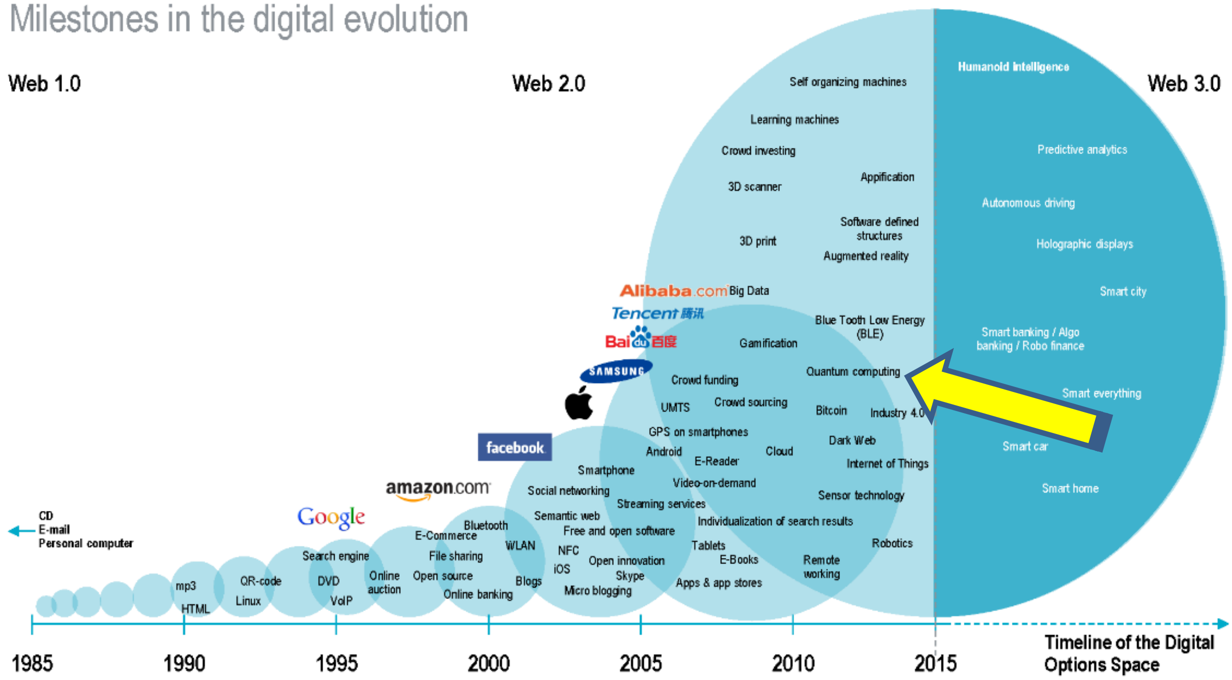
Increasingly, innovations are reaching significant diffusion milestones faster

Time from introducing a product to an adoption rate of 25% across US citizens [years]



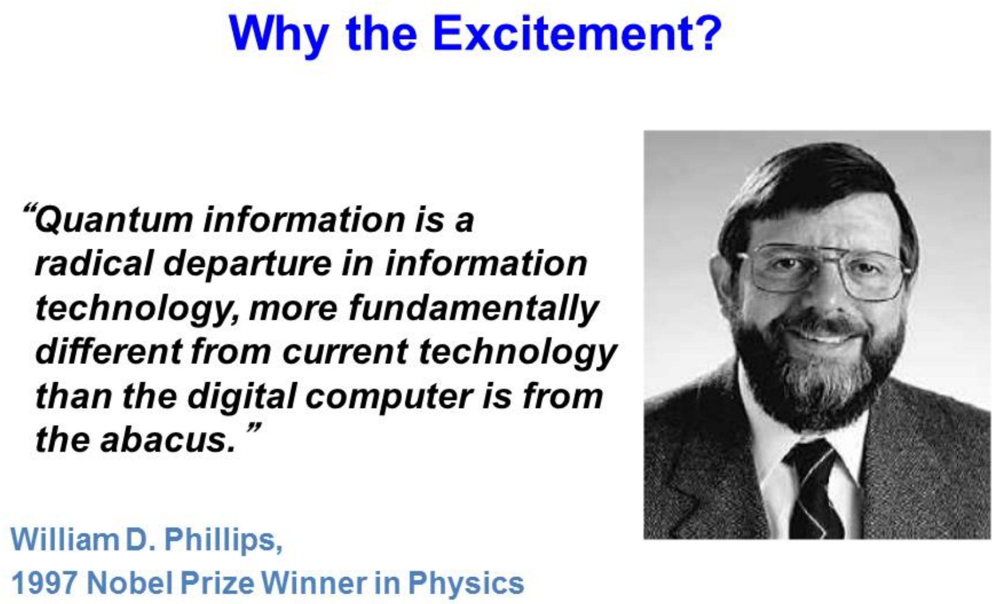
Digital Transformation has changed everything and is set to continue, as digital options follow an exponential growth path

Milestones in the digital evolution

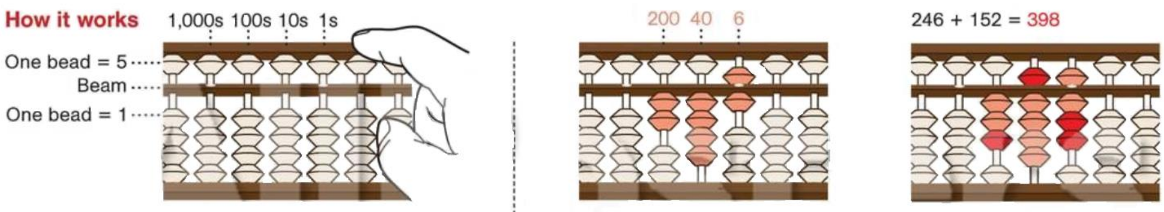


Programming Languages and Compilers for Quantum Computers [15]

Overview



[15] Programming Languages and Compilers for Quantum Computers; Columbia University Computer Science. Obtained via the web in December 2018.



An abacus can be used to add, subtract, multiply, and divide. Each rod represents a power of ten.

Moving a bead toward the beam adds value. The position of the beads represents a number—in this case 246.

To add 152, add one to the hundreds rod, five to the tens rod, and two to the units rod, for a sum of 398.

Scientists find a way to enhance the performance of quantum computers [16]

Overview

- Advantage gained by acquiring the first computer that renders all other computers obsolete would be enormous and bestow economic, military, and public health advantages to the winner.
- Scientists worldwide have yet to achieve a "quantum advantage – the point where a quantum computer outperforms a conventional computer on any task.
- The University of Southern California (USC) is the only university in the world with a quantum computer; its 1098-qubit D-Wave quantum annealer specializes in solving optimization problems.
    - Part of the USC-Lockheed Martin Center for Quantum Computing, it is located at USC's Information Sciences Institute.
        - However, the latest research findings were achieved not on the D-Wave machine, but on smaller scale, general-purpose quantum computers: IBM's 16-qubit QX5 and Rigetti's 19-qubit Acorn.

[16] Scientists find a way to enhance the performance of quantum computers. University of Southern California (USC) – November 29, 2018. Obtained via the web in December 2018.

- The quest for quantum computing supremacy is a geopolitical priority for Europe, China, Canada, Australia, and the United States.
- Congress is considering two new bills to establish the United States as a leader in quantum computing.
    - In September, the House of Representatives passed the National Quantum Initiative Act to allocate $1.3 billion in five years to spur research and development.
        - It would create a National Quantum Coordination Office in the White House to supervise research nationwide.
        - A separate bill, the Quantum Computing Research Act by Sen. Kamala Harris, D-Calif., directs the Department of Defense to lead a quantum computing effort.

List of Companies Involved in Quantum Computing [17]

Overview

- Booz Allen Hamilton (BAH) of Tysons Corner, VA initiated quantum computing involvement supporting computing in 2015.

Booz | Allen | Hamilton
strategy and technology consultants

- Northrop Grumman (NG) of West Falls Church, VA initiated quantum computing involvement supporting the area of computing.

NORTHROP GRUMMAN

[17] List of companies involved in quantum computing by Wikipedia. Obtained via the web in December 2018.

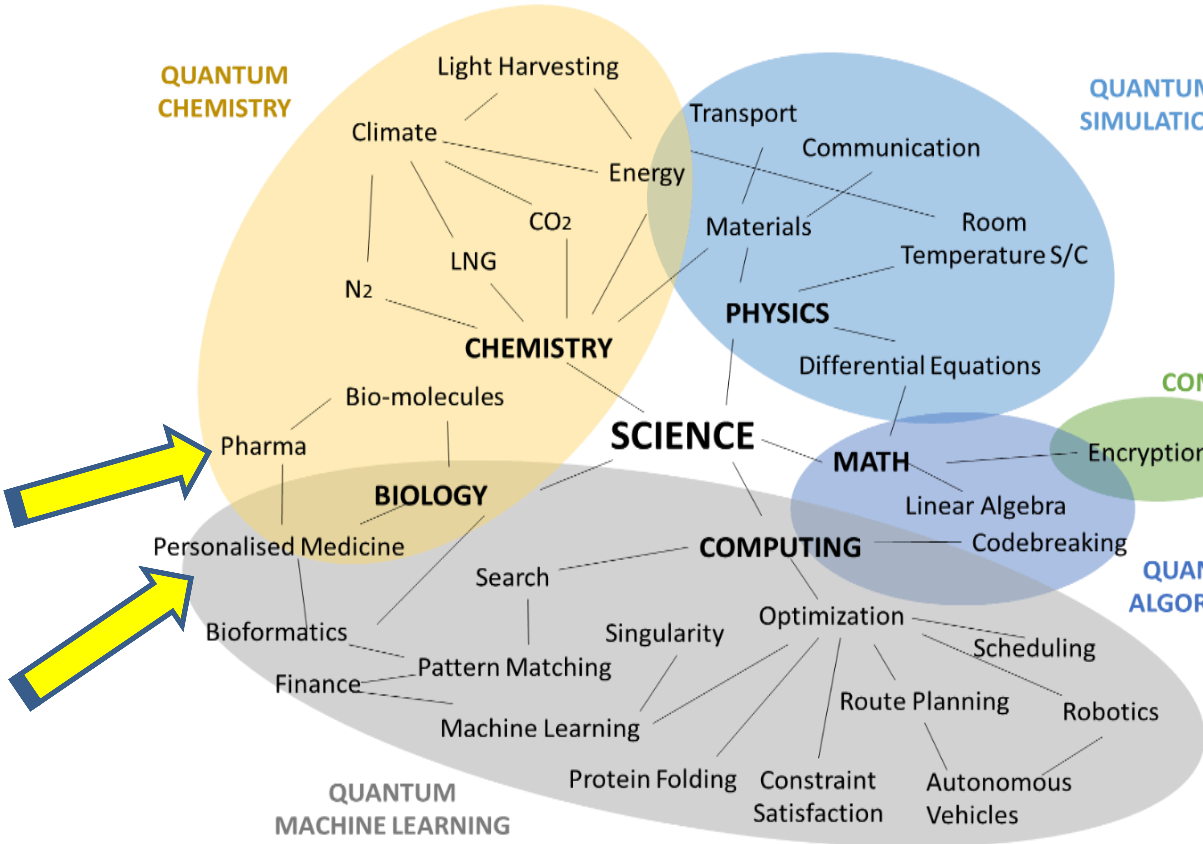
- QxBranch of Washington, DC initiated quantum computing involvement supporting computing in 2014.

- ionQ of College Park, MD initiated quantum computing involvement in conjunction with the University of Maryland and Duke University in the computing area of ions.

- Lockheed Martin of Bethesda, MD initiated quantum computing involvement in conjunction with the University of Southern California (USC) and the University College London.

- Nokia Bell Labs of Murray Hill, NJ initiated quantum computing involvement in conjunction with the University of Oxford in the area of computing.
- And many more…


Global Quantum Computing Market
By 24 National Markets
U.S.A.
Canada
Mexico
Brazil
Rest of Latin America
UK
France
Netherlands
Denmark, Sweden, Norway, Finland
Germany
Switzerland
Russia
Rest of Europe
Saudi Arabia
Other GCC
Israel
South Africa
Rest of ME&A
India
China
Japan
Singapore
Australia
Rest of Asia Pacific
By 4 Sectors
National Security
Government
Gov. Funded RDT&E
Industry & Business Sectors
By 17 Vertical Markets
Defense & Intelligence
Homeland Security & Public Safety
Government & Public Services
Gov. Funded RDT&E
Banking & Securities
Manufacturing & Logistics
Insurance
Healthcare & Pharmaceutical
Retail & Wholesale
Information Technology Industry
Telecommunication
Automotive, Aerospace & Transportation
Energy & Utilities
Web, Media & Entertainment
Smart Cities
Other Vertical Markets
Cybersecurity
By 4 Revenue Sources
Systems Sales
Software Sales
QC as a Service
Government Funded RDT&E
By 4 Regional Markets
North America
Europe
Asia Pacific
ROW

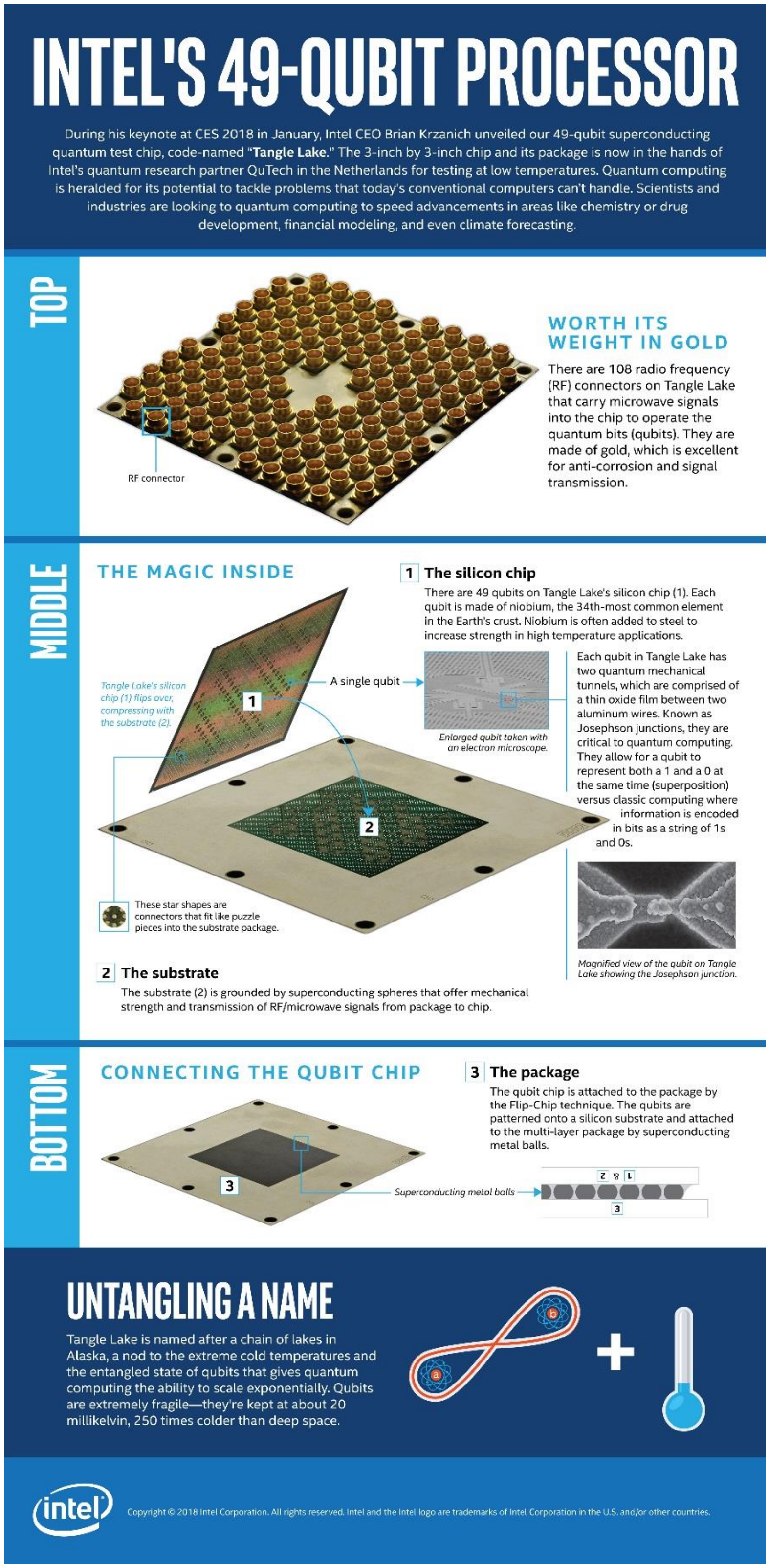

QUANTUM CHEMISTRY
Light Harvesting
Climate
Energy
CO2
LNG
N2
CHEMISTRY
QUANTUM SIMULATION
Transport
Communication
Materials
Room Temperature S/C
PHYSICS
Differential Equations
QUANTUM COMMUNICATION
Encryption
Bio-molecules
Pharma
SCIENCE
MATH
BIOLOGY
Linear Algebra
Personalised Medicine
COMPUTING
Codebreaking
QUANTUM ALGORITHMS
Search
Optimization
Bioformatics
Singularity
Scheduling
Pattern Matching
Finance
Route Planning
Robotics
Machine Learning
Protein Folding
Constraint Satisfaction
Autonomous Vehicles
QUANTUM MACHINE LEARNING

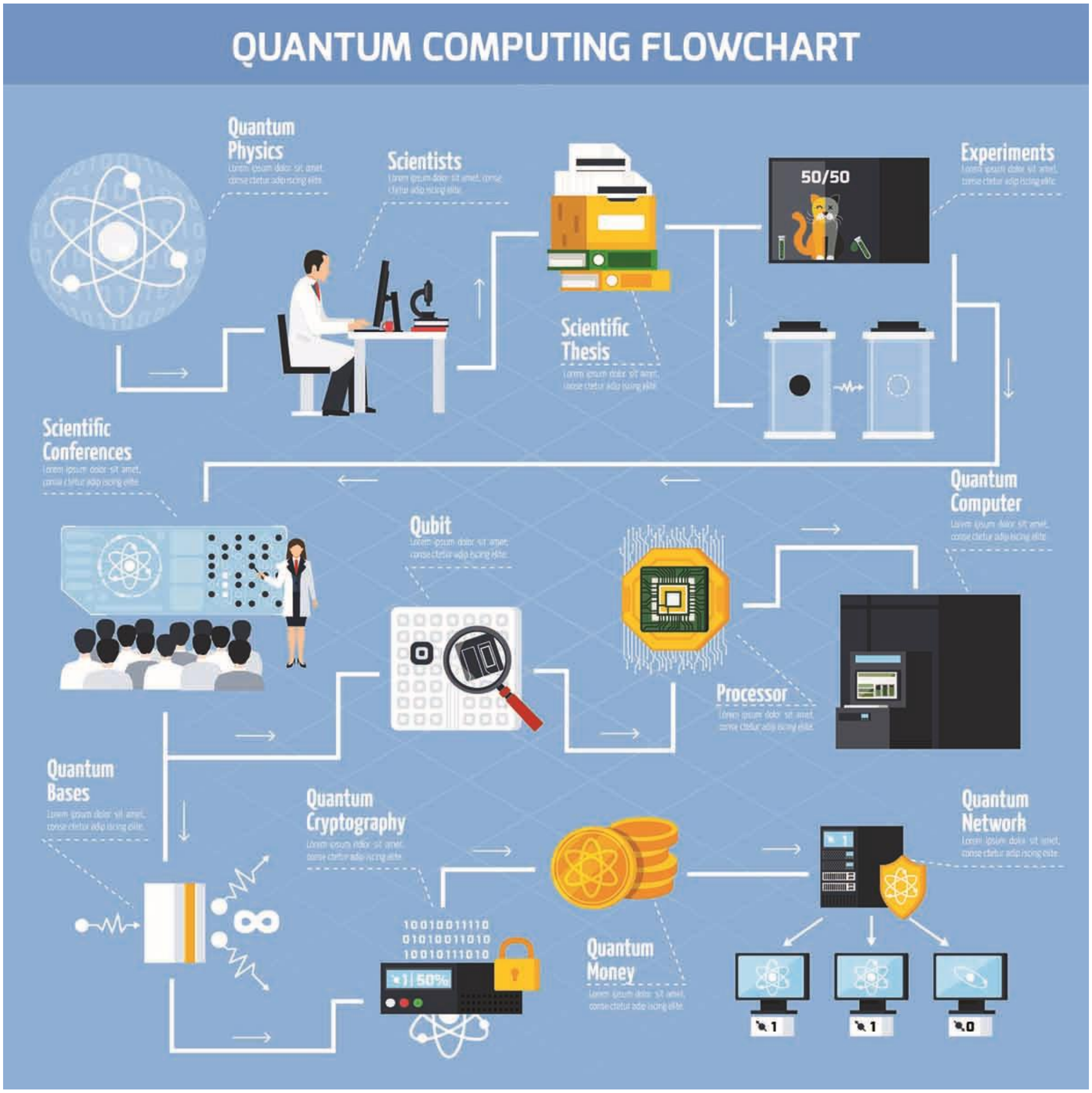
Pictorial Insight of Quantum Computing [18]

[18] Obtained through various sources as found on the World Wide Web / Internet through January 2019.

Overview

- The following graphics are provided to assist with understanding quantum computers at a basic level.
    - It is understood that some graphics may not help one's understanding at all.
    - Viewer discretion is advised.


INTEL'S 49-QUBIT PROCESSOR
During his keynote at CES 2018 in January, Intel CEO Brian Krzanich unveiled our 49-qubit superconducting quantum test chip, code-named "Tangle Lake." The 3-inch by 3-inch chip and its package is now in the hands of Intel's quantum research partner QuTech in the Netherlands for testing at low temperatures. Quantum computing is heralded for its potential to tackle problems that today's conventional computers can't handle. Scientists and industries are looking to quantum computing to speed advancements in areas like chemistry or drug development, financial modeling, and even climate forecasting.
TOP
RF connector
WORTH ITS WEIGHT IN GOLD
There are 108 radio frequency (RF) connectors on Tangle Lake that carry microwave signals into the chip to operate the quantum bits (qubits). They are made of gold, which is excellent for anti-corrosion and signal transmission.
MIDDLE
THE MAGIC INSIDE
Tangle Lake's silicon chip (1) flips over, compressing with the substrate (2).
A single qubit
1
2
These star shapes are connectors that fit like puzzle pieces into the substrate package.
1 The silicon chip
There are 49 qubits on Tangle Lake's silicon chip (1). Each qubit is made of niobium, the 34th-most common element in the Earth's crust. Niobium is often added to steel to increase strength in high temperature applications.
Enlarged qubit taken with an electron microscope.
Each qubit in Tangle Lake has two quantum mechanical tunnels, which are comprised of a thin oxide film between two aluminum wires. Known as Josephson junctions, they are critical to quantum computing. They allow for a qubit to represent both a 1 and a 0 at the same time (superposition) versus classic computing where information is encoded in bits as a string of 1s and 0s.
Magnified view of the qubit on Tangle Lake showing the Josephson junction.
2 The substrate
The substrate (2) is grounded by superconducting spheres that offer mechanical strength and transmission of RF/microwave signals from package to chip.
BOTTOM
CONNECTING THE QUBIT CHIP
3
Superconducting metal balls
3 The package
The qubit chip is attached to the package by the Flip-Chip technique. The qubits are patterned onto a silicon substrate and attached to the multi-layer package by superconducting metal balls.
UNTANGLING A NAME
Tangle Lake is named after a chain of lakes in Alaska, a nod to the extreme cold temperatures and the entangled state of qubits that gives quantum computing the ability to scale exponentially. Qubits are extremely fragile—they're kept at about 20 millikelvin, 250 times colder than deep space.
a
b
+
intel
Copyright © 2018 Intel Corporation. All rights reserved. Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.


QUANTUM COMPUTING FLOWCHART
Quantum Physics
Scientists
Scientific Thesis
Experiments
50/50
Scientific Conferences
Quantum Computer
Qubit
Processor
Quantum Bases
Quantum Cryptography
10010011110
01010011010
10010111010
50%
Quantum Money
Quantum Network

A QUANTUM COMPUTING PRIMER

intel

Quantum computers are different from the digital computing that drives today's data centers, cloud environments, PCs and other devices. Digital computation requires data to be encoded into binary digits (bits), each of which is always in one of two definite states (0 or 1). However, quantum computation uses quantum bits (qubits), which can be in multiple states simultaneously. As a result, operations on qubits can amount to a large number of calculations in parallel. It has been shown that in theory, some specific problems should be solvable in much less time on a quantum computer than using the best known algorithms for a conventional computer. Here are four key concepts that are the foundation of quantum computing.

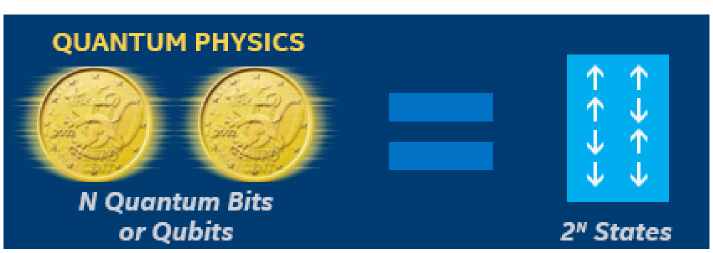
1 SUPERPOSITION

Think of classical physics as a coin. It can be either heads or tails. If it were a bit, it would be 0 or 1. In quantum physics, this coin is best thought of as a constantly spinning coin. It represents heads and tails simultaneously. As a result, a **qubit** would be both 0 and 1 and spin simultaneously up and down.

Quantum state: a simultaneous representation of multiple classical states.

2 ENTANGLEMENT

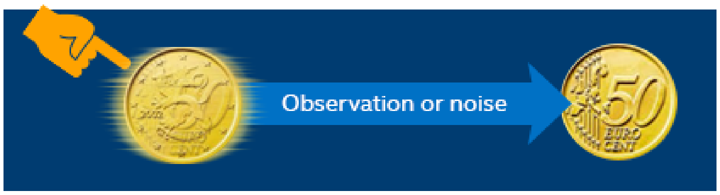
Entanglement gives quantum computing the ability to scale exponentially. If one qubit simultaneously represents two states, two qubits represents four states when coupled together. They can no longer be treated independently; they now form a **coupled**, or **entangled, super state**. As more qubits link together, the number of states exponentially increase, which could lead to a computer with astronomically large computing power.



The **two qubits** can no longer be treated independently. They form a **super state**.

3 FRAGILITY

Quantum states are quite **fragile**. If you measure, observe, touch, or perturb any of these states, they collapse to a classical state. The states don't stick around for very long, which is why quantum computers are currently hard to build.



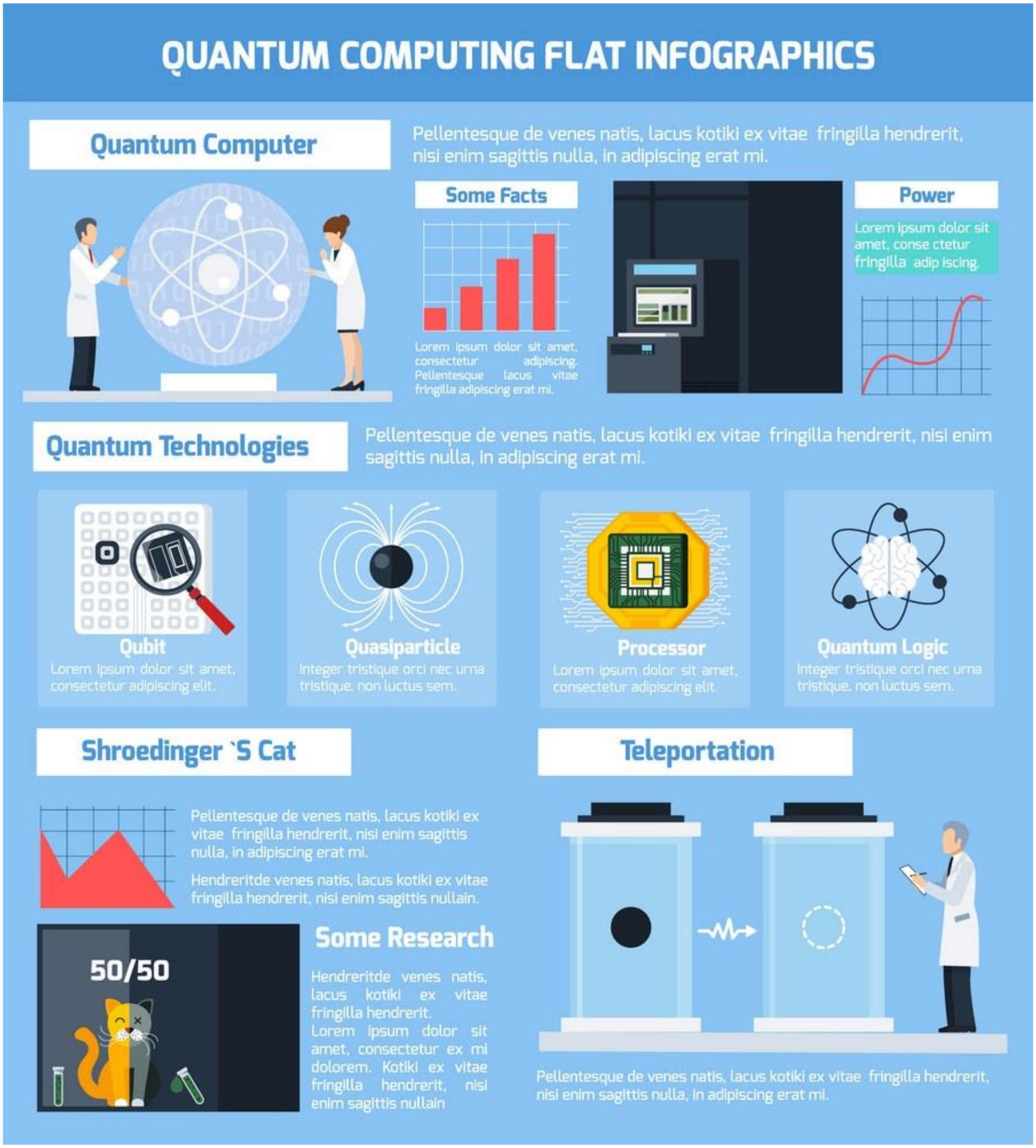
A **quantum state** collapses to a classical state if disturbed by noise or measurement.

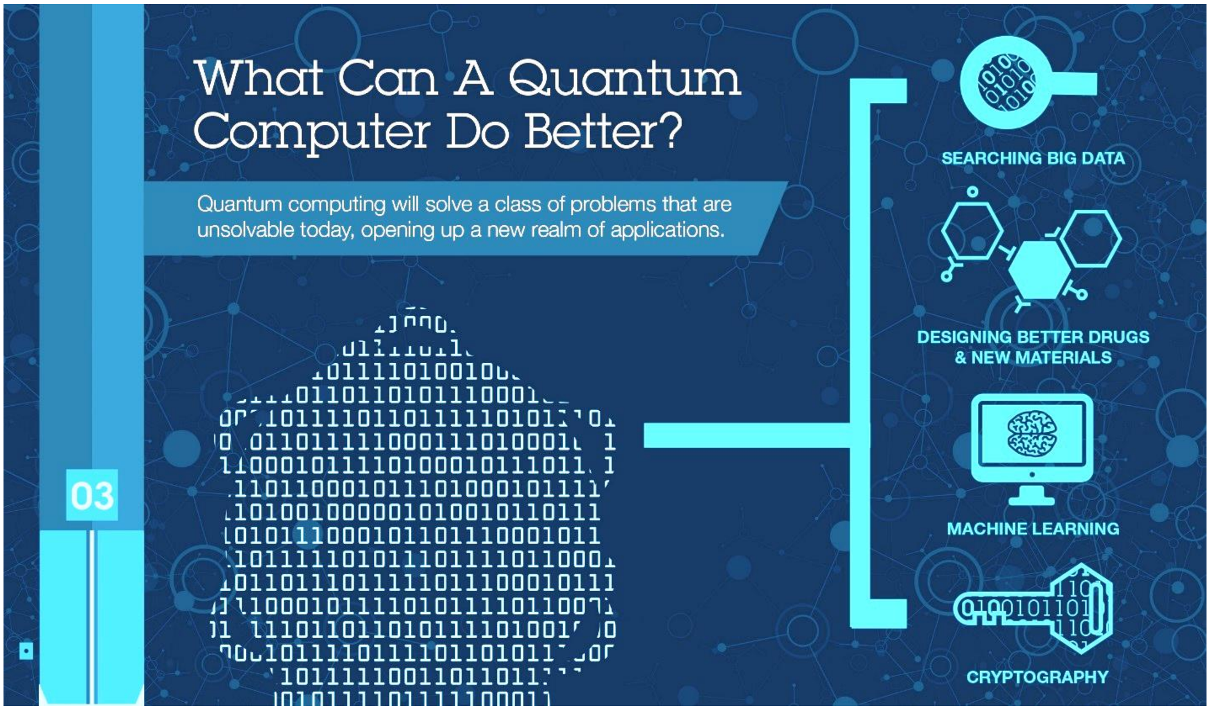
4 NO CLONING

A corollary to fragility is the '**No Cloning Theorem**.' In classical physics, if two bits are represented by the coins below, one can copy or eavesdrop and recreate the information. In contrast, the information entangled within a set of qubits will be lost if someone tries to observe or copy them. A quantum state cannot be copied without the sender or receiver realizing this. This concept serves as the basis of quantum communications.

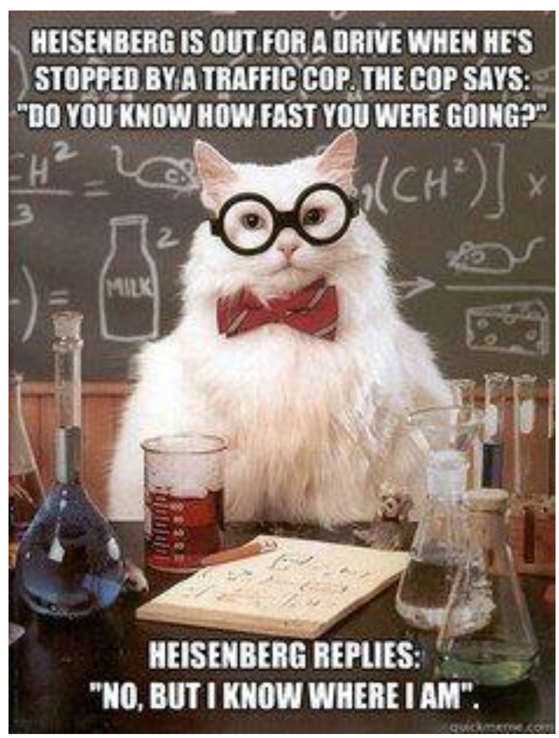
One **cannot** copy, intercept or steal without ruining a quantum state.

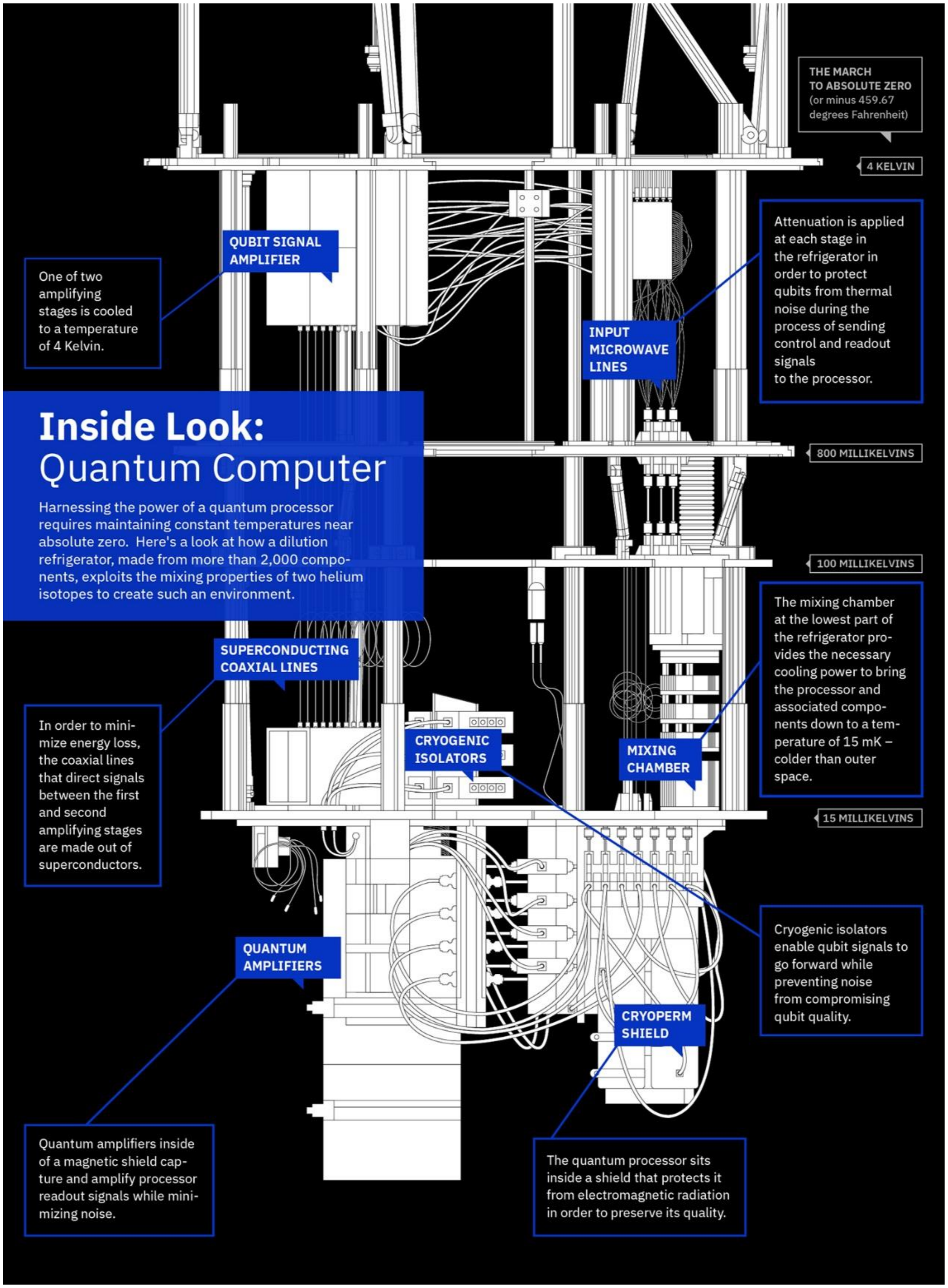
Quantum computing holds a credible promise of radically enhanced performance, with the potential to solve specific complex problems that are practically unsolvable by today's computers. Development of actual quantum computers is still in its infancy, but quantum computing has the potential to solve complex simulations such as large-scale financial analysis and more effective drug development.


QUANTUM COMPUTING FLAT INFOGRAPHICS
Quantum Computer
Pellentesque de venes natis, lacus kotiki ex vitae fringilla hendrerit, nisi enim sagittis nulla, in adipiscing erat mi.
Some Facts
Lorem ipsum dolor sit amet, consectetur adipiscing. Pellentesque lacus vitae fringilla adipiscing erat mi.
Power
Lorem ipsum dolor sit amet, conse ctetur fringilla adip iscing.
Quantum Technologies
Pellentesque de venes natis, lacus kotiki ex vitae fringilla hendrerit, nisi enim sagittis nulla, in adipiscing erat mi.
Qubit
Lorem ipsum dolor sit amet, consectetur adipiscing elit.
Quasiparticle
Integer tristique orci nec urna tristique, non luctus sem.
Processor
Lorem ipsum dolor sit amet, consectetur adipiscing elit.
Quantum Logic
Integer tristique orci nec urna tristique, non luctus sem.
Shroedinger `S Cat
Pellentesque de venes natis, lacus kotiki ex vitae fringilla hendrerit, nisi enim sagittis nulla, in adipiscing erat mi.
Hendreritde venes natis, lacus kotiki ex vitae fringilla hendrerit, nisi enim sagittis nullain.
50/50
Some Research
Hendreritde venes natis, lacus kotiki ex vitae fringilla hendrerit. Lorem ipsum dolor sit amet, consectetur ex mi dolorem. Kotiki ex vitae fringilla hendrerit, nisi enim sagittis nullain
Teleportation
Pellentesque de venes natis, lacus kotiki ex vitae fringilla hendrerit, nisi enim sagittis nulla, in adipiscing erat mi.



The uncertainty principle.
Werner Heisenberg famously discovered that when you measure the position (let's sayyyy) of an electron as precisely as you can, you find yourself more and more in the dark about its momentum. And vice versa. You can pin down one or the other, but not both.




THE MARCH TO ABSOLUTE ZERO (or minus 459.67 degrees Fahrenheit)
4 KELVIN
QUBIT SIGNAL AMPLIFIER
One of two amplifying stages is cooled to a temperature of 4 Kelvin.
INPUT MICROWAVE LINES
Attenuation is applied at each stage in the refrigerator in order to protect qubits from thermal noise during the process of sending control and readout signals to the processor.
Inside Look: Quantum Computer
Harnessing the power of a quantum processor requires maintaining constant temperatures near absolute zero. Here's a look at how a dilution refrigerator, made from more than 2,000 components, exploits the mixing properties of two helium isotopes to create such an environment.
800 MILLIKELVINS
100 MILLIKELVINS
SUPERCONDUCTING COAXIAL LINES
In order to minimize energy loss, the coaxial lines that direct signals between the first and second amplifying stages are made out of superconductors.
CRYOGENIC ISOLATORS
MIXING CHAMBER
The mixing chamber at the lowest part of the refrigerator provides the necessary cooling power to bring the processor and associated components down to a temperature of 15 mK – colder than outer space.
15 MILLIKELVINS
QUANTUM AMPLIFIERS
Cryogenic isolators enable qubit signals to go forward while preventing noise from compromising qubit quality.
CRYOPERM SHIELD
Quantum amplifiers inside of a magnetic shield capture and amplify processor readout signals while minimizing noise.
The quantum processor sits inside a shield that protects it from electromagnetic radiation in order to preserve its quality.

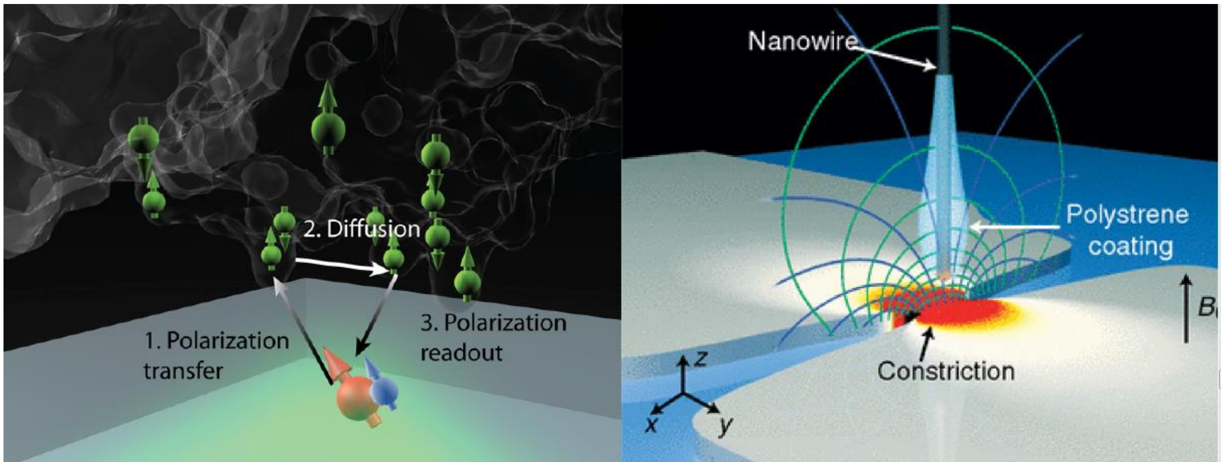


Figure 15. *(left)* **NV centers embedded a few nanometers under a diamond surface are being developed as ultra-sensitive magnetic field probes of external materials, including nuclear magnetic resonance detection of single proteins** *(Credit: P Cappellaro, MIT; R Walsworth, M Lukin, H Park, Harvard). (right)* **An alternative method, magnetic resonance force detection with nanoscale cantilevers, is being developed for nanometer-scale nuclear magnetic resonance imaging.** *(credit: Raffi Budakian, U. Waterloo)* [19]

Figure 14. Quantum hardware is being deployed in space. In 2016, China launched a special-purpose satellite for quantum secure communications *(left).* **Space-based quantum networks could enable new forms of quantum global positioning systems and ultra-precise measurements** *(right).* [20]

[19] Future Directions of Quantum Information Processing. A workshop on the emerging science and technology of quantum computation, communication, and measurement. Virginia Tech Applied Research Corporation (VT-ARC) – August 26, 2016. Obtained from the web in December 2018.
[20] Ibid.

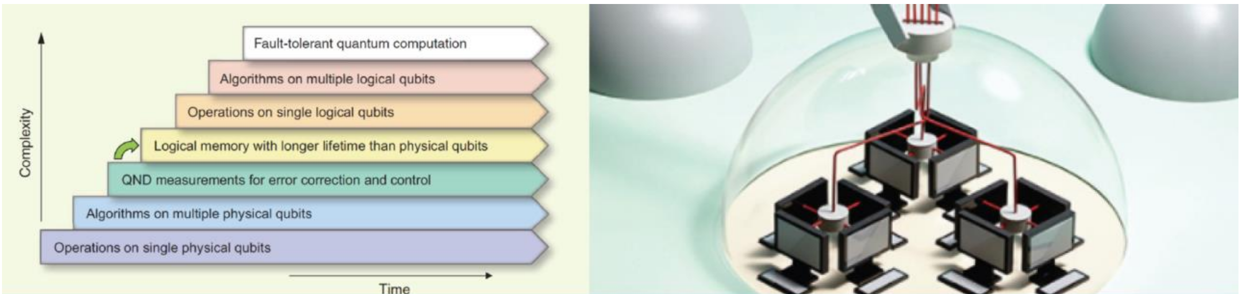


Figure 12. *(left)* **To develop fault-tolerant quantum computation requires mastery of increasingly sophisticated technologies. Quantum algorithms and quantum nondemolition measurements on few qubits are possible today. Logical qubit encoding with performance better than the physical constituent qubits will likely be accomplished in the next five years.** *(Credit: Devoret and Schoelkopf, Science 339, 1169 (2013)) (Right)* **A focus is on the architectures that will efficiently link quantum memories into networks and modular quantum computers.** *(Image credit: C. Monroe, R. Schoelkopf, and M. Lukin / Scientific American, 2016)*

[21]

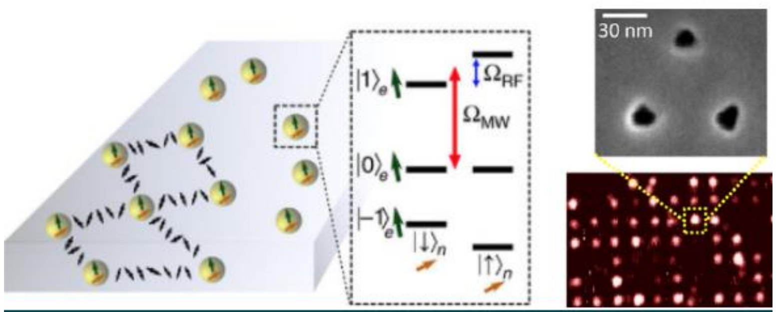


Figure 11. Arrays of NV-centers in diamond, closely enough spaced so that electron spins interact magnetically, are promising for mid-scale quantum computers that could even function at room temperature. The image on the left shows a schematic of the required architecture *(Image credit: N. Yao, NComm, 2012)***; it is now becoming possible to reach the required length scales experimentally** *(D. Scarabelli, Nano Letters, 2016).* [22]

[21] Ibid.
[22] Ibid.

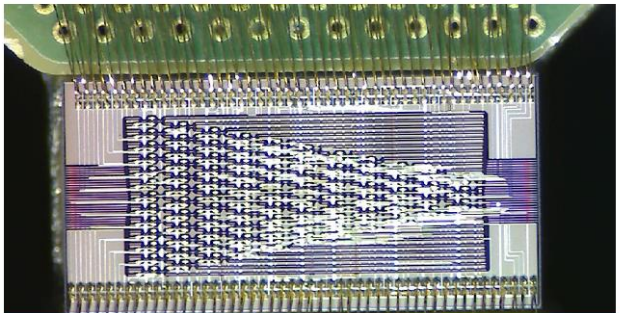


Figure 9. Programmable Photonic Integrated Circuits (PICs) allow precision control of tens to hundreds of photonic waveguides with near-perfect phase stability, building on modern silicon electronics processing. Programmable PICs are being used for quantum communications, machine learning, and have been proposed as an early system to demonstrate "quantum supremacy" by boson sampling. *(Image Credit: MIT, AFRL, OPSIS)* [23]

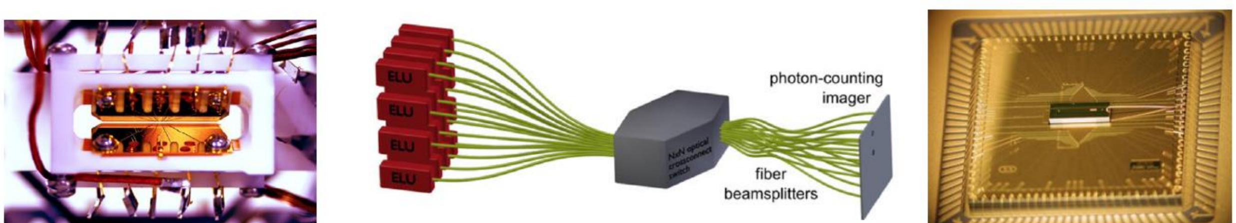


Figure 7.*(left)* **A small programmable (5-qubit) trapped ion quantum computer. (Monroe group, University of Maryland and Joint Quantum Institute).** *(center)* **Photonic interconnects to connect quantum memory modules (***Credit: Kenneth R Brown, Jungsang Kim & Christopher Monroe). (right)* **Advanced microfabricated ion traps from Sandia National Laboratories** *(Image courtesy of Duke University).*

24

[23] Ibid.
[24] Ibid.

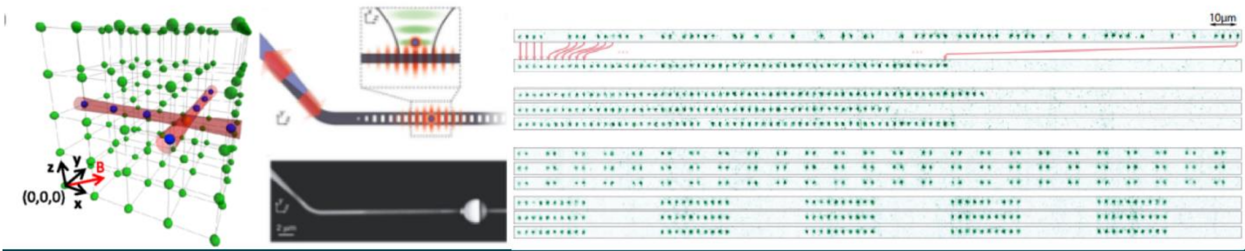


Figure 5. *(left)* **Ultracold atoms can now be assembled in 3D lattices where they can be addressed by laser beams, as shown here as a 5x5x5 array of neutral atoms** *(Credit: D.S. Weiss group, Penn State). (center)* **An alternative approach consists of nanophotonic device interfaces. Shown here is a photonic crystal nanocavity whose evanescent field can be coupled to an individual ^{87}Rb atom (blue circle). A tapered fiber connected to the cavity allows efficient coupling to fiber optics.***(right)* **Regular 1D and 2D arrays of individually controlled atoms were recently assembled using optical tweezers with real-time feedback.** *(Credit for b and c: Lukin, Greiner, and Vuletic groups at Harvard and MIT).*

[25]

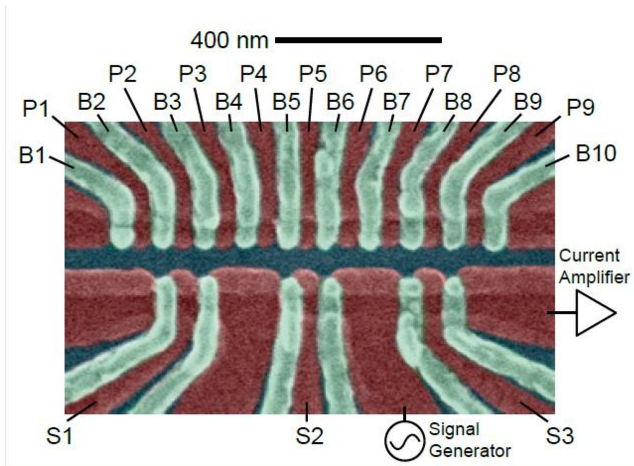


Figure 6. Nanoscale device to control 12 semiconductor quantum dots in an undoped Si/SiGe heterostructure. *(Credit: David Zajac, Petta Group, Princeton University)* [26]

[25] Ibid.
[26] Ibid.

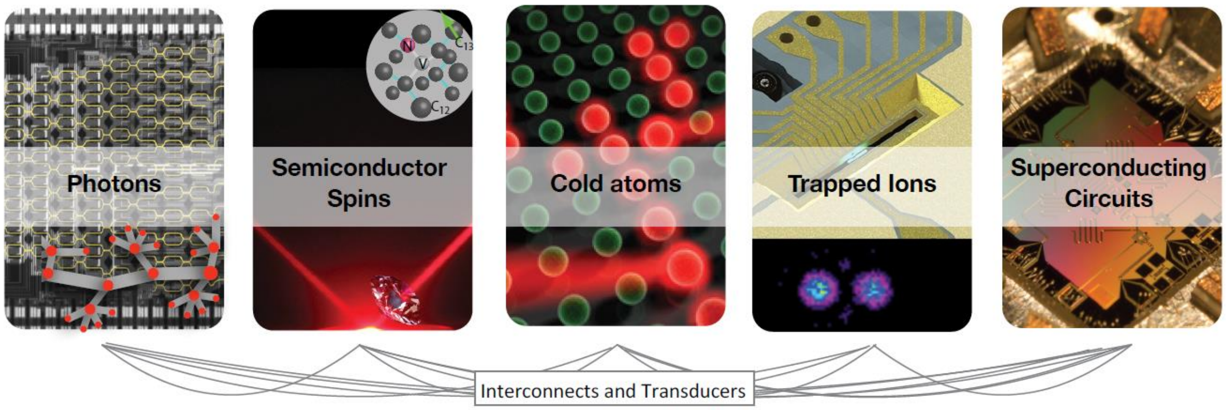


Figure 3. Leading physical platforms for quantum information processing include photons, spins in semiconductors, ultracold atoms, trapped ions, and superconducting circuits. A major area of research also focuses on connecting these platforms, which often requires the development of transducers to photonic states, which can travel long distances with little decoherence.

[27]

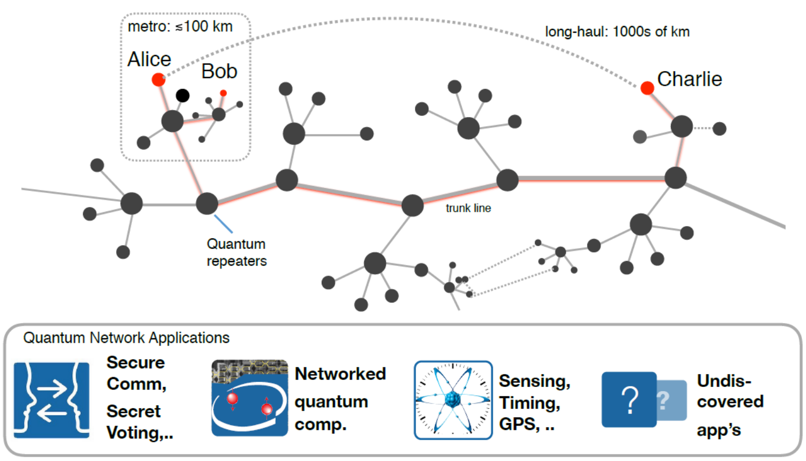


Figure 13. Quantum key distribution (QKD) allows unconditionally secure communication between two users, Alice and Bob, but its reach is limited to the metro-scale because of photon loss. Long-range quantum communications will become possible with the introduction of quantum repeater nodes in trunk lines that could span vast distances. These connected quantum memories will form a "quantum network" layer on top of today's classical internet. This "quantum internet" will allow a host of new proposed technologies beyond secure quantum communications, no doubt including many still undiscovered applications.

[28]

[27] Ibid.
[28] Ibid.

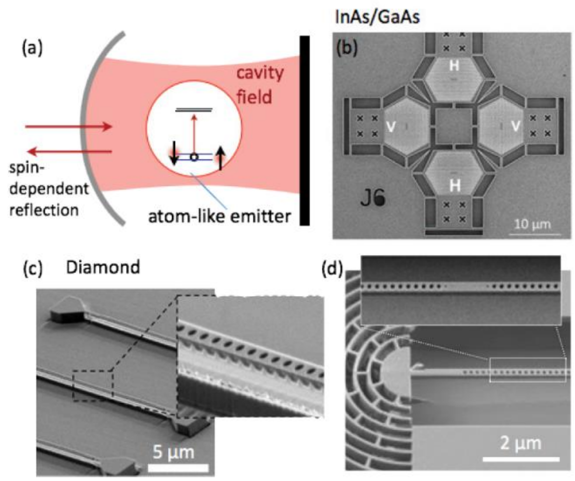


Figure 10. Optical cavities can act as efficient interfaces between incident photons and atom-like quantum memories *(a)*. **Such interfaces based on photonic crystal cavities are being used to link quantum memories in photonic circuits.** *(b)* **Cavity-waveguide networks for InAs/GaAs quantum dots.** *(Credit: Waks group, University of Maryland).* *(c)* **Diamond cavity-waveguide systems with triangular** *(bottom left)* **and** *(d)* **rectangular** *(bottom right)* **nanobeams for NV and SiV memories.** *(MIT and Harvard)*

[29]

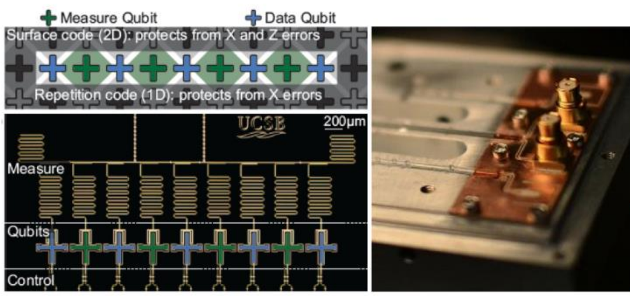
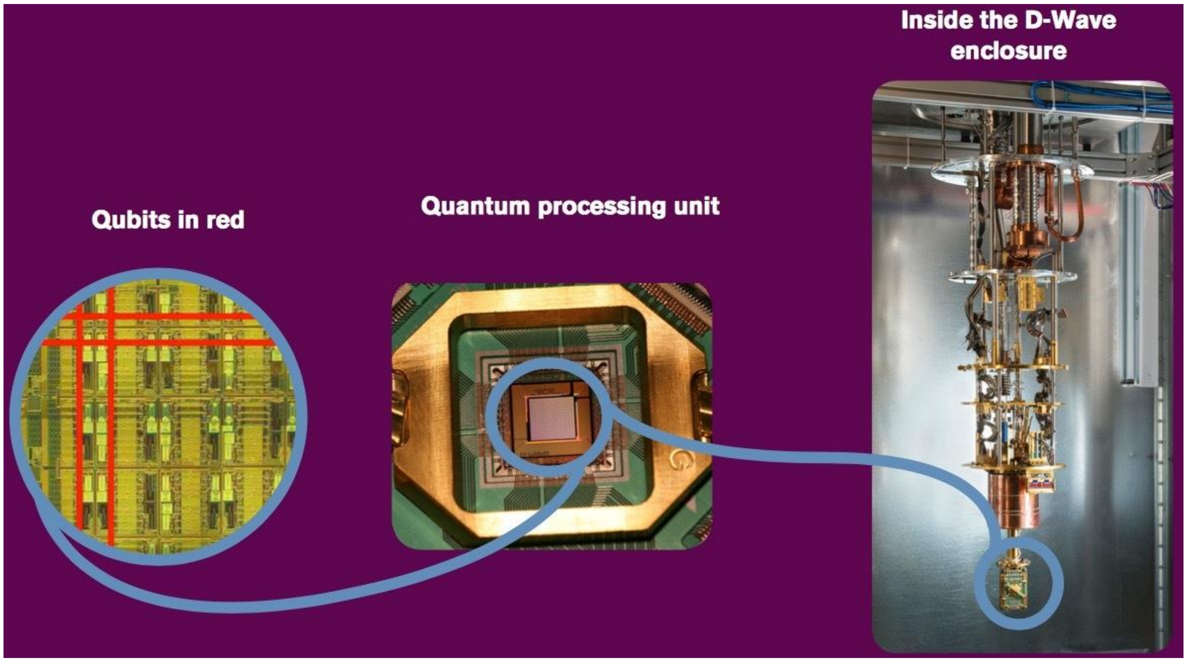
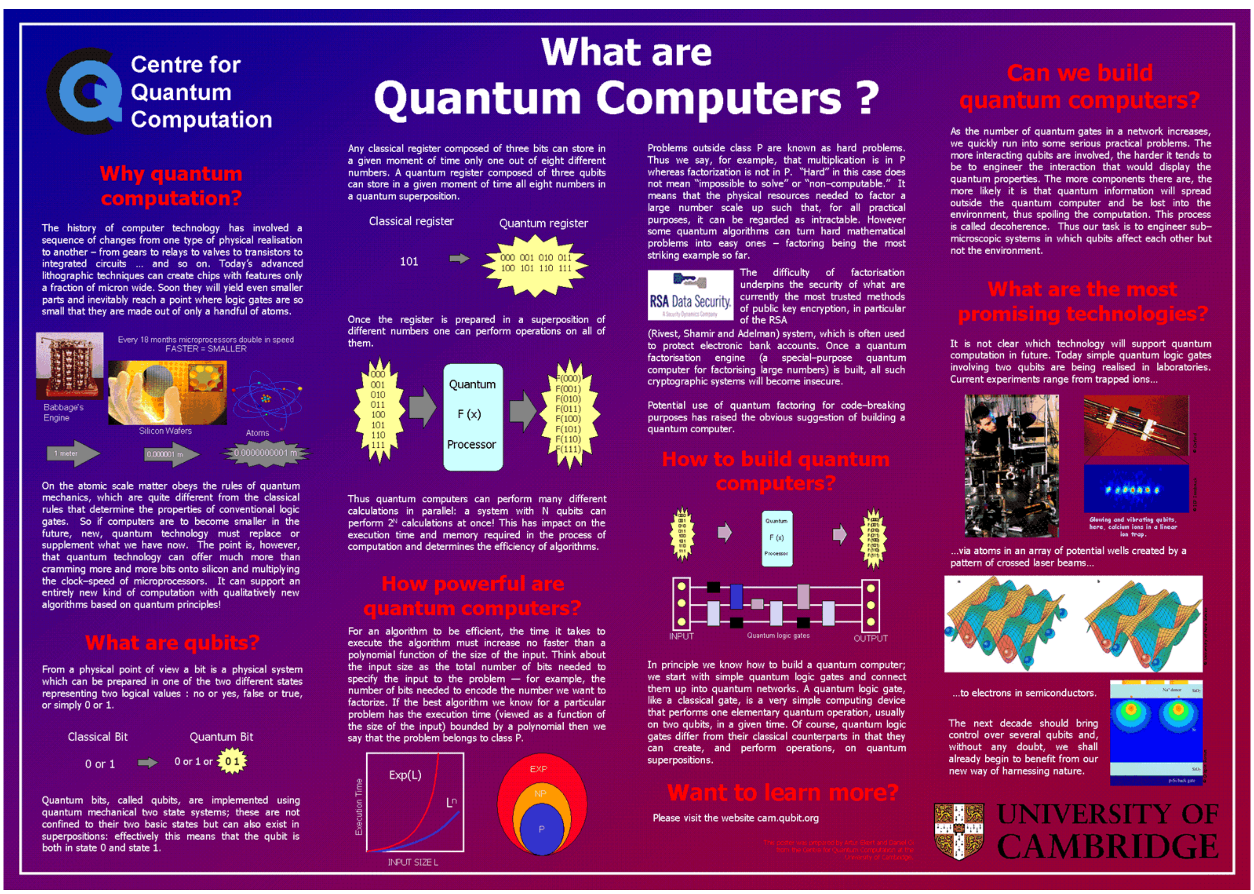


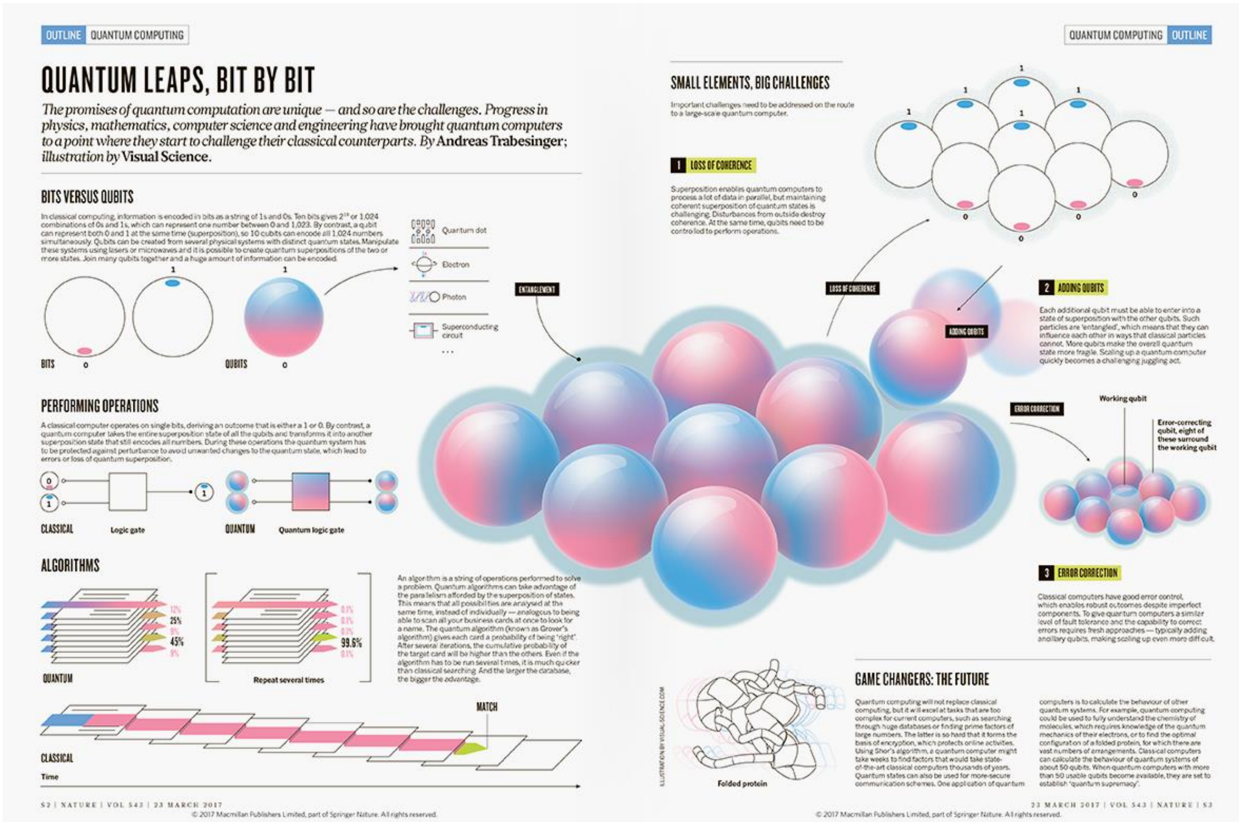
Figure 4. Superconducting quantum computing approaches. *(left)* **Circuit-model computing approach with 9 qubits for error correction** *(Martinis group, Google).* *(right)* **3D cavities have enable record coherence times and error correction** *(Yale).*

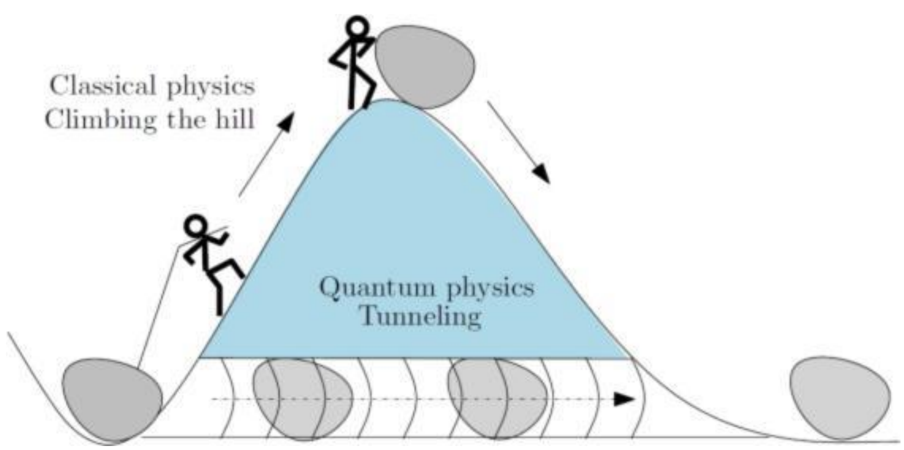
[30]

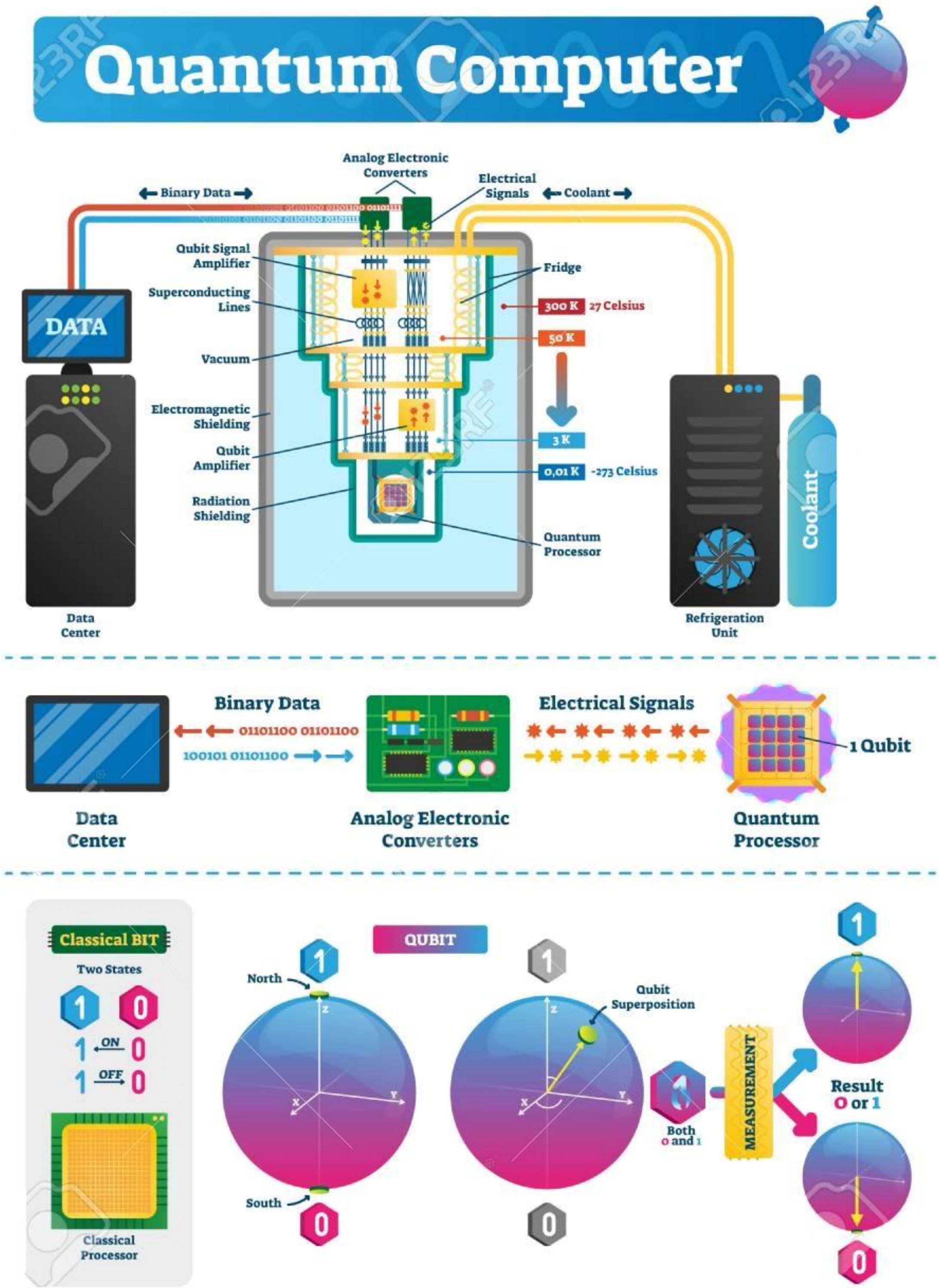
[29] Ibid.
[30] Ibid.


Inside the D-Wave enclosure
Qubits in red
Quantum processing unit


Centre for Quantum Computation
What are Quantum Computers ?
Why quantum computation?
The history of computer technology has involved a sequence of changes from one type of physical realisation to another – from gears to relays to valves to transistors to integrated circuits ... and so on. Today's advanced lithographic techniques can create chips with features only a fraction of micron wide. Soon they will yield even smaller parts and inevitably reach a point where logic gates are so small that they are made out of only a handful of atoms.
Every 18 months microprocessors double in speed
FASTER = SMALLER
Babbage's Engine
Silicon Wafers
Atoms
1 meter
0.000001 m
0.0000000001 m
On the atomic scale matter obeys the rules of quantum mechanics, which are quite different from the classical rules that determine the properties of conventional logic gates. So if computers are to become smaller in the future, new, quantum technology must replace or supplement what we have now. The point is, however, that quantum technology can offer much more than cramming more and more bits onto silicon and multiplying the clock–speed of microprocessors. It can support an entirely new kind of computation with qualitatively new algorithms based on quantum principles!
What are qubits?
From a physical point of view a bit is a physical system which can be prepared in one of the two different states representing two logical values : no or yes, false or true, or simply 0 or 1.
Classical Bit
Quantum Bit
0 or 1
0 or 1 or 0 1
Quantum bits, called qubits, are implemented using quantum mechanical two state systems; these are not confined to their two basic states but can also exist in superpositions: effectively this means that the qubit is both in state 0 and state 1.
Any classical register composed of three bits can store in a given moment of time only one out of eight different numbers. A quantum register composed of three qubits can store in a given moment of time all eight numbers in a quantum superposition.
Classical register
Quantum register
101
000 001 010 011 100 101 110 111
Once the register is prepared in a superposition of different numbers one can perform operations on all of them.
000 001 010 011 100 101 110 111
Quantum F (x) Processor
F(000) F(001) F(010) F(011) F(100) F(101) F(110) F(111)
Thus quantum computers can perform many different calculations in parallel: a system with N qubits can perform 2^N calculations at once! This has impact on the execution time and memory required in the process of computation and determines the efficiency of algorithms.
How powerful are quantum computers?
For an algorithm to be efficient, the time it takes to execute the algorithm must increase no faster than a polynomial function of the size of the input. Think about the input size as the total number of bits needed to specify the input to the problem — for example, the number of bits needed to encode the number we want to factorize. If the best algorithm we know for a particular problem has the execution time (viewed as a function of the size of the input) bounded by a polynomial then we say that the problem belongs to class P.
Exp(L)
L^n
Execution Time
INPUT SIZE L
EXP
NP
P
Problems outside class P are known as hard problems. Thus we say, for example, that multiplication is in P whereas factorization is not in P. "Hard" in this case does not mean "impossible to solve" or "non–computable." It means that the physical resources needed to factor a large number scale up such that, for all practical purposes, it can be regarded as intractable. However some quantum algorithms can turn hard mathematical problems into easy ones – factoring being the most striking example so far.
RSA Data Security.
A Security Dynamics Company
The difficulty of factorisation underpins the security of what are currently the most trusted methods of public key encryption, in particular of the RSA (Rivest, Shamir and Adelman) system, which is often used to protect electronic bank accounts. Once a quantum factorisation engine (a special–purpose quantum computer for factorising large numbers) is built, all such cryptographic systems will become insecure.
Potential use of quantum factoring for code–breaking purposes has raised the obvious suggestion of building a quantum computer.
How to build quantum computers?
Quantum F (x) Processor
INPUT
Quantum logic gates
OUTPUT
In principle we know how to build a quantum computer; we start with simple quantum logic gates and connect them up into quantum networks. A quantum logic gate, like a classical gate, is a very simple computing device that performs one elementary quantum operation, usually on two qubits, in a given time. Of course, quantum logic gates differ from their classical counterparts in that they can create, and perform operations, on quantum superpositions.
Want to learn more?
Please visit the website cam.qubit.org
This poster was prepared by Artur Ekert and Daniel Oi from the Centre for Quantum Computation at the University of Cambridge.
Can we build quantum computers?
As the number of quantum gates in a network increases, we quickly run into some serious practical problems. The more interacting qubits are involved, the harder it tends to be to engineer the interaction that would display the quantum properties. The more components there are, the more likely it is that quantum information will spread outside the quantum computer and be lost into the environment, thus spoiling the computation. This process is called decoherence. Thus our task is to engineer sub–microscopic systems in which qubits affect each other but not the environment.
What are the most promising technologies?
It is not clear which technology will support quantum computation in future. Today simple quantum logic gates involving two qubits are being realised in laboratories. Current experiments range from trapped ions...
Glowing and vibrating qubits, here, calcium ions in a linear ion trap.
...via atoms in an array of potential wells created by a pattern of crossed laser beams...
...to electrons in semiconductors.
The next decade should bring control over several qubits and, without any doubt, we shall already begin to benefit from our new way of harnessing nature.
UNIVERSITY OF CAMBRIDGE


OUTLINE QUANTUM COMPUTING
QUANTUM LEAPS, BIT BY BIT
The promises of quantum computation are unique — and so are the challenges. Progress in physics, mathematics, computer science and engineering have brought quantum computers to a point where they start to challenge their classical counterparts. By Andreas Trabesinger; illustration by Visual Science.
BITS VERSUS QUBITS
PERFORMING OPERATIONS
ALGORITHMS
SMALL ELEMENTS, BIG CHALLENGES
1 LOSS OF COHERENCE
2 ADDING QUBITS
3 ERROR CORRECTION
GAME CHANGERS: THE FUTURE
QUANTUM COMPUTING OUTLINE


Classical physics
Climbing the hill
Quantum physics
Tunneling


Quantum Computer
Analog Electronic Converters
Binary Data
Electrical Signals
Coolant
Qubit Signal Amplifier
Superconducting Lines
Vacuum
Electromagnetic Shielding
Qubit Amplifier
Radiation Shielding
Fridge
300 K 27 Celsius
50 K
3 K
0,01 K -273 Celsius
Quantum Processor
DATA
Data Center
Refrigeration Unit
Coolant
Binary Data
01101100 01101100
100101 01101100
Electrical Signals
1 Qubit
Data Center
Analog Electronic Converters
Quantum Processor
Classical BIT
Two States
1 0
1 ON 0
1 OFF 0
Classical Processor
QUBIT
North
South
1
0
Qubit Superposition
Both 0 and 1
MEASUREMENT
Result 0 or 1

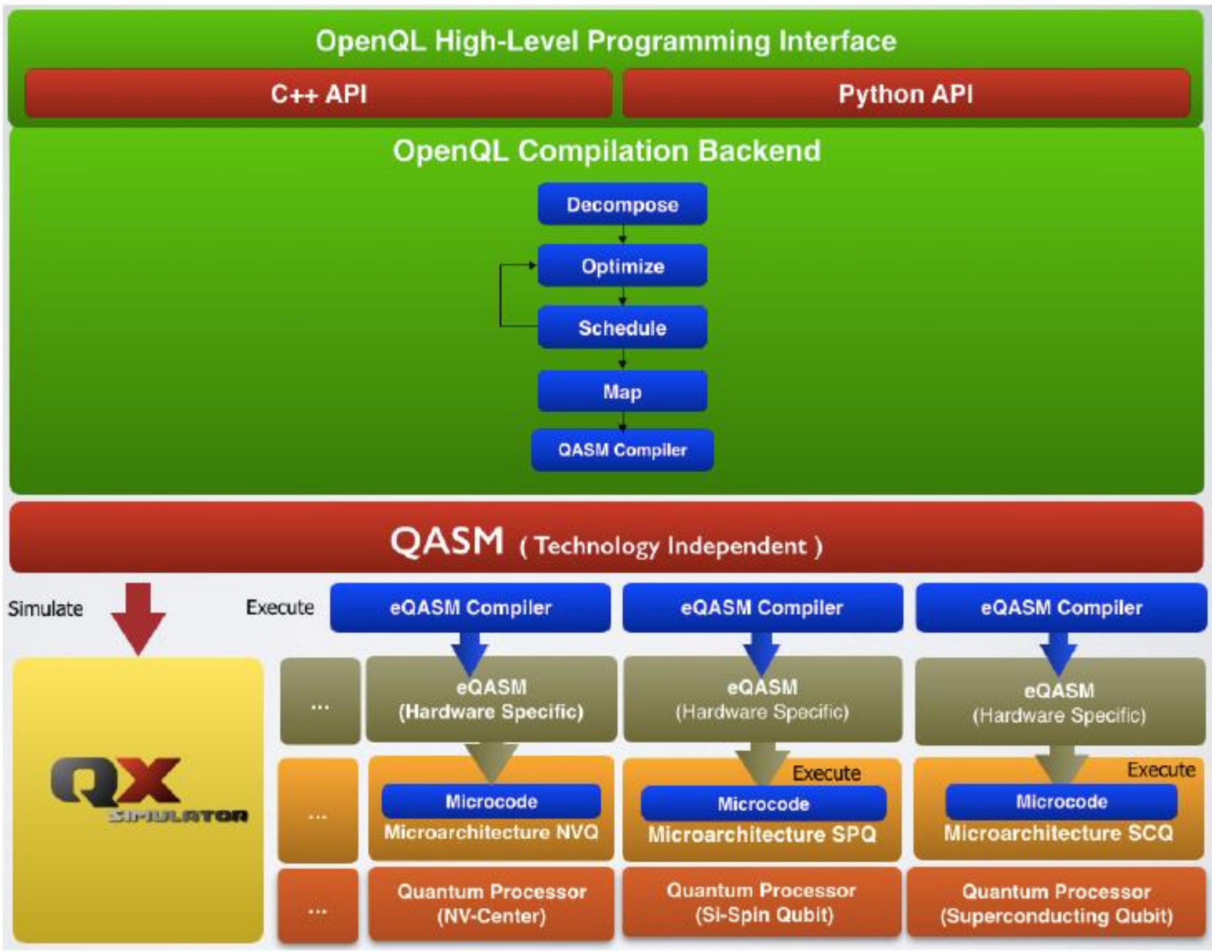
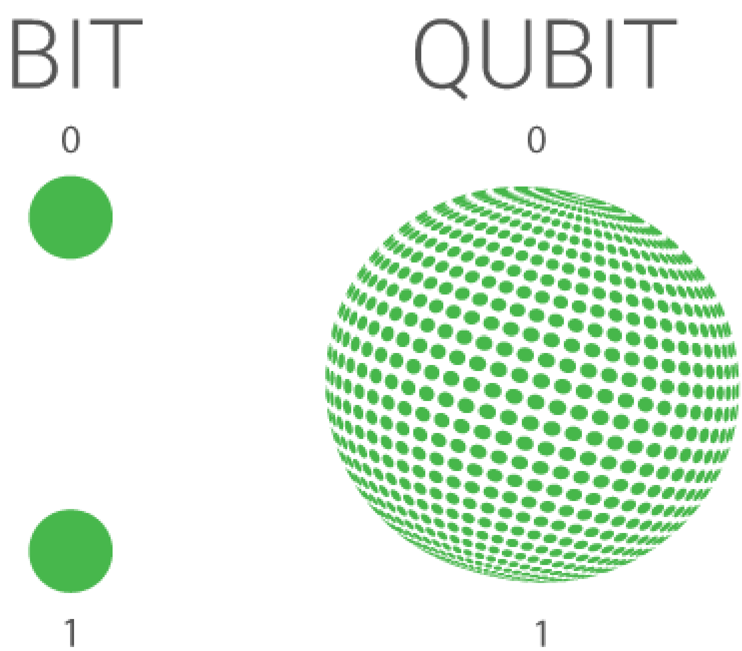
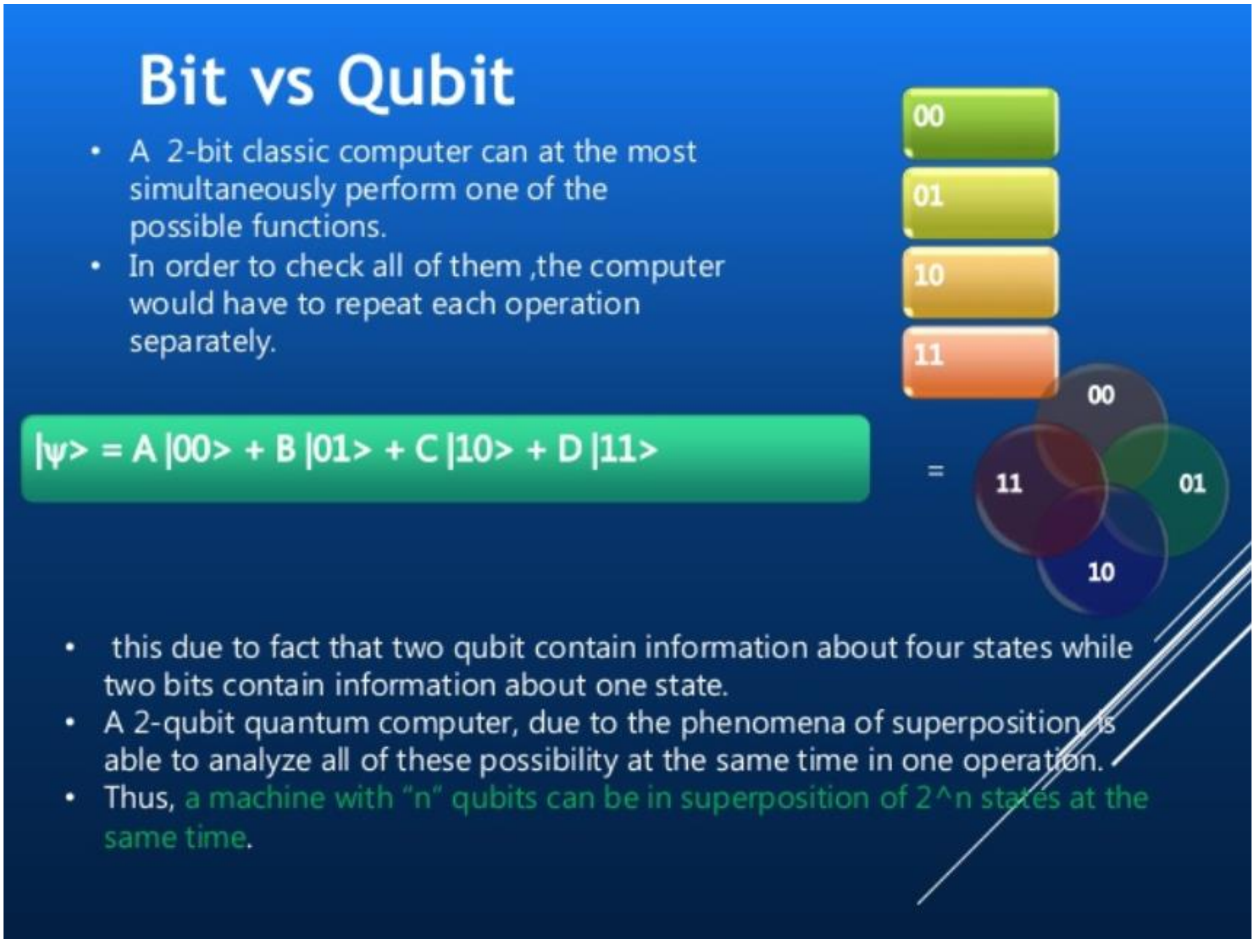
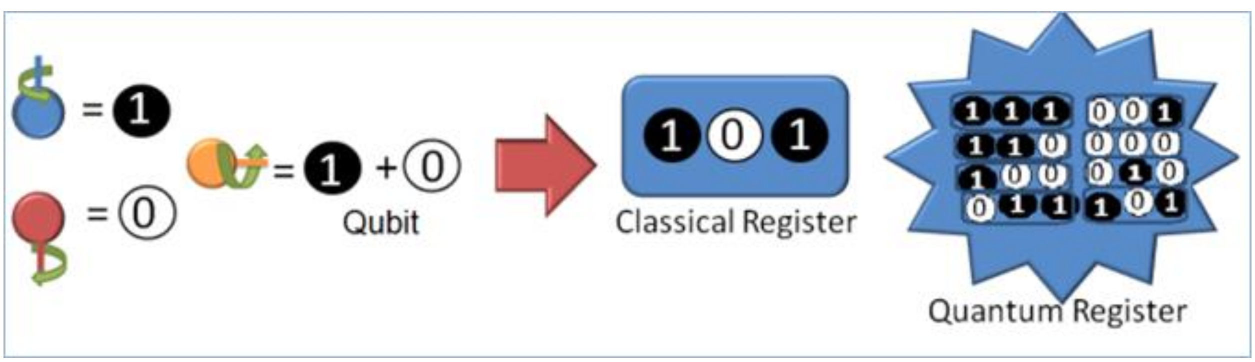


Figure 4.1: OpenQL high-level programming interface


Classical Bit
1 Bit
N Bit
0
1
or
0 0 1 1 0
Either 0 or 1
One out of 2N possible permutations
Quantum Bit
1 Bit
N Bit
α|0⟩+β|1⟩
a1|0000···0⟩+a2|1100···0⟩+a3|1110···0⟩ + ··· + a2N|1111···1⟩
Both 0 and 1
All of 2N possible permutations


BIT
QUBIT
0
1
0
1


Bit vs Qubit
• A 2-bit classic computer can at the most simultaneously perform one of the possible functions.
• In order to check all of them ,the computer would have to repeat each operation separately.
00
01
10
11
|ψ> = A |00> + B |01> + C |10> + D |11>
=
00
11
01
10
• this due to fact that two qubit contain information about four states while two bits contain information about one state.
• A 2-qubit quantum computer, due to the phenomena of superposition is able to analyze all of these possibility at the same time in one operation.
• Thus, a machine with "n" qubits can be in superposition of 2^n states at the same time.


= 1
= 0
= 1 + 0
Qubit
1 0 1
Classical Register
Quantum Register

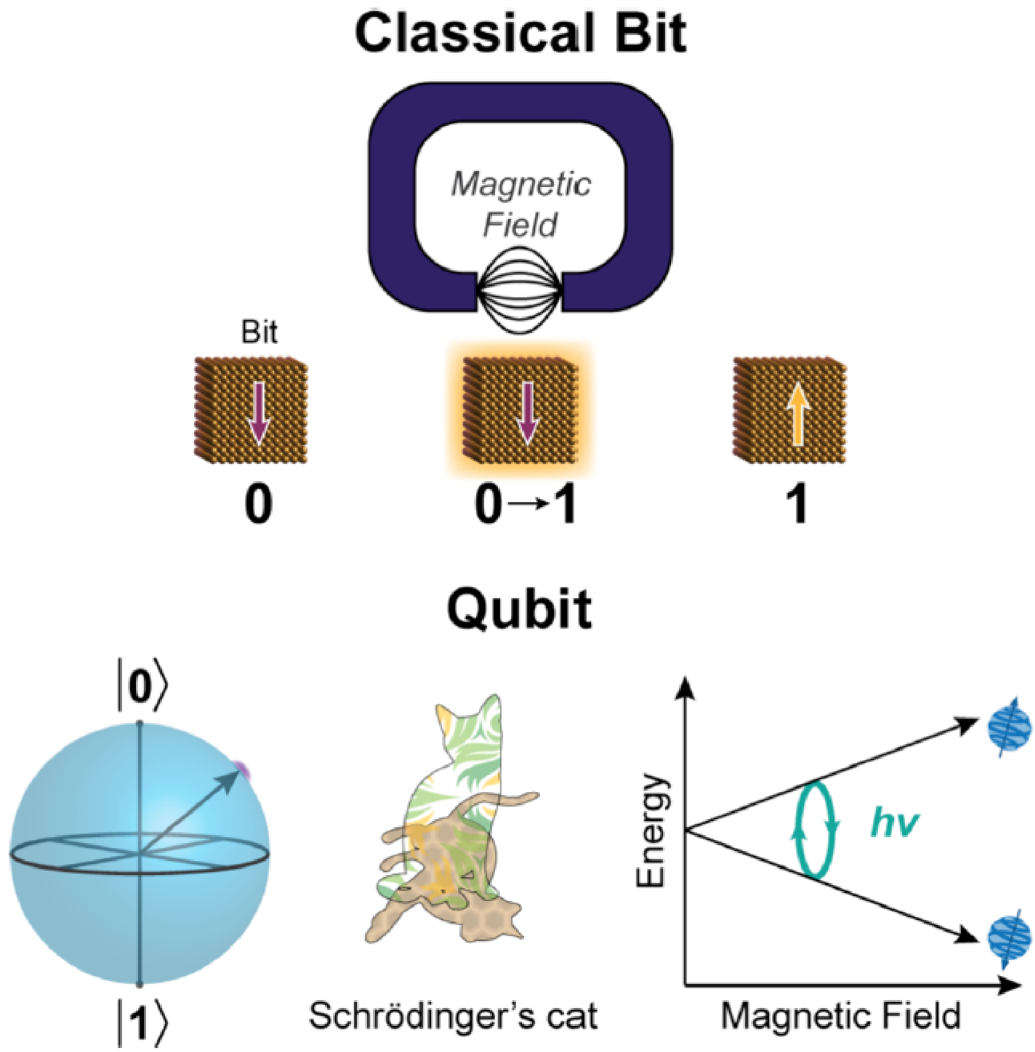
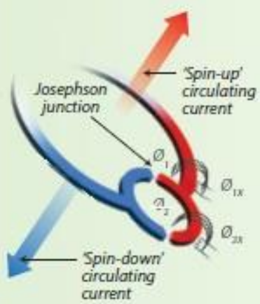


Figure 1. Schematic diagram depicting the contrast between a classical bit and a quantum bit (qubit). Top: a magnetic read–write head flipping the orientation of a macroscopic (classical) magnetic bit. Bottom: various representations of a qubit. Left: the Bloch sphere represents all possible qubit superposition states. Center: Schrödinger's cat serves as a common, albeit flawed, analogy for the "dead and alive" nature of a qubit superposition. Right: electron spins in a magnetic field can be placed into a superposition between two spin sublevels via pulsed microwaves.

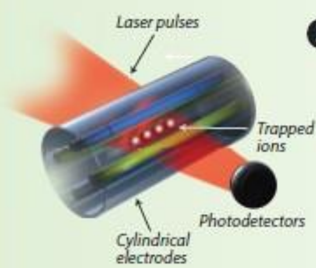
Four routes to quantum computing

Physicists are developing different flavors of quantum computer, based on different types of quantum bits (qubits).

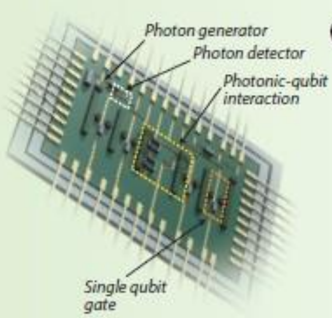
1 Spin qubits
Made from spins of electrons or nuclei trapped in a solid substrate, such as nitrogen vacancy centers in diamond. Can remain in superposition states for up to several seconds and can be compatible with current chip-manufacturing technology. Noise from solid-state environment could hamper scaling up.



2 Superconducting circuits
Superpositions of currents flowing in opposite directions around a superconductor at the same time. Being solid state, they are potentially easy to manufacture, but have relatively short coherence times and require low temperatures to operate.



3 Ion traps
Qubits reside in arrays of ions trapped in electric fields, with their quantum states manipulated by lasers. Very clean systems that don't suffer from defects, allowing for logic gates with low error rates—but scaling up will require new fabrication infrastructure.



4 Photonic circuits
Qubits are encoded in the quantum states of photons travelling around circuits in silicon chips, which include etched waveguides and tiny linear optical components. Need for qubit redundancy could be minimized by photons' resistance to interference, but building photonic logic gates is difficult, and single-photon sources pose a technical challenge.

Illustration by Phil Saunders

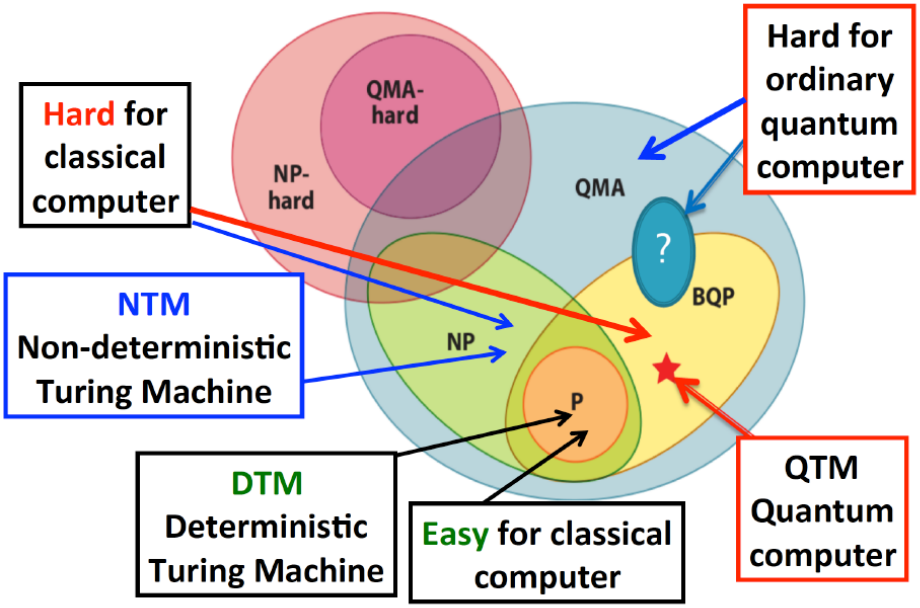
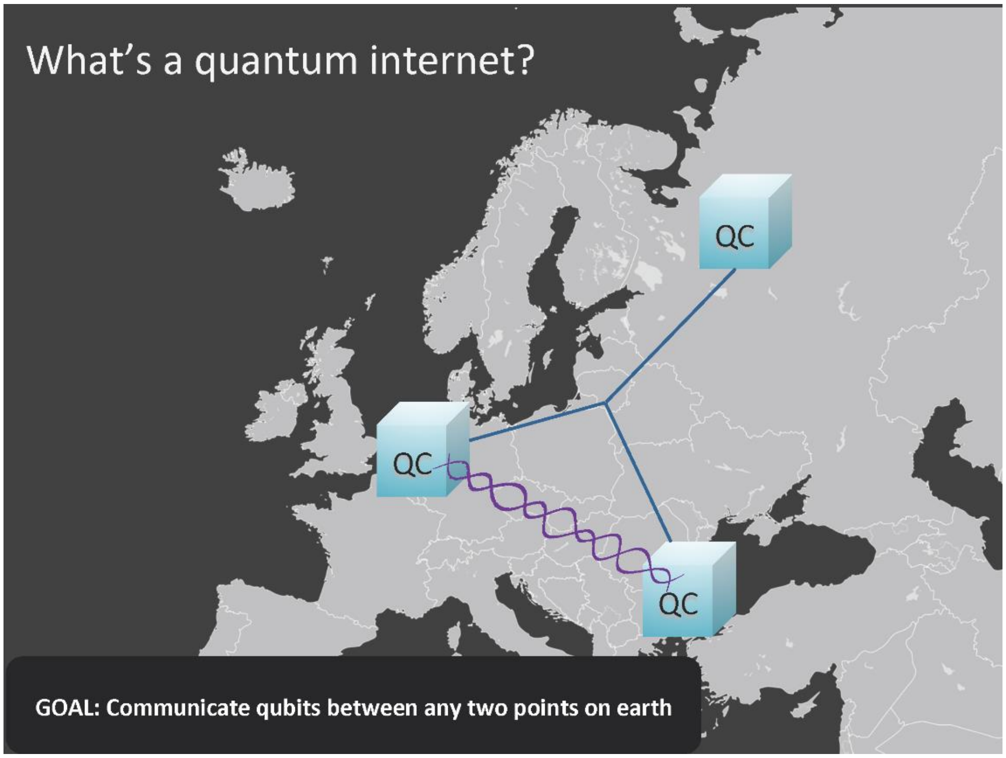
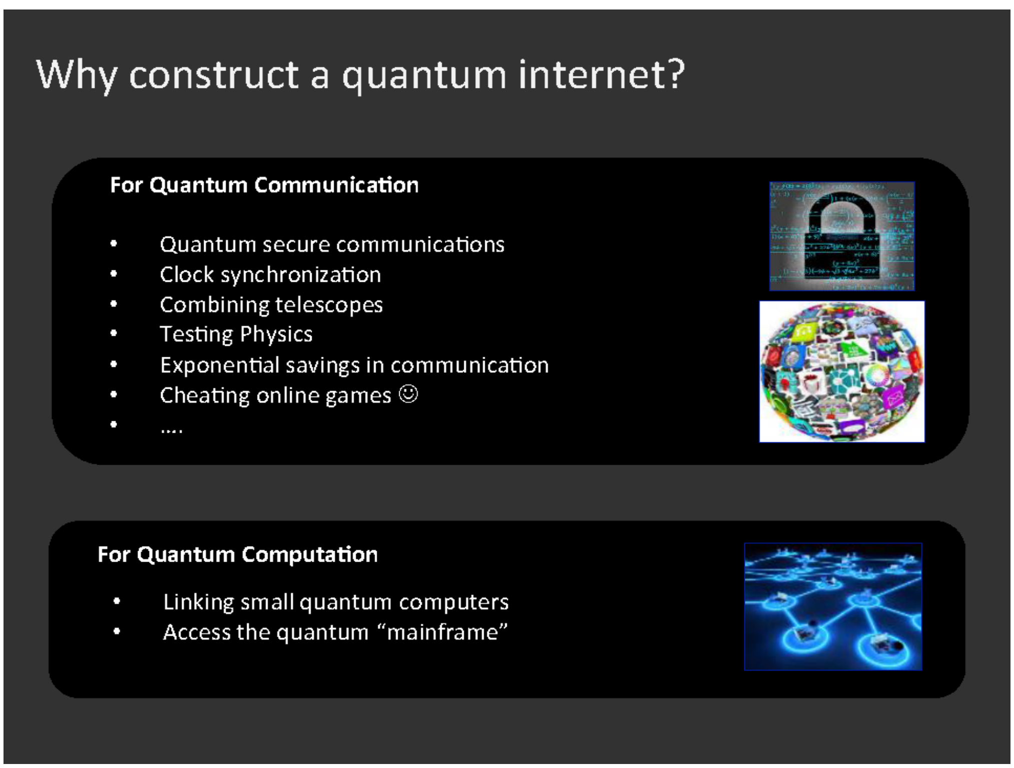
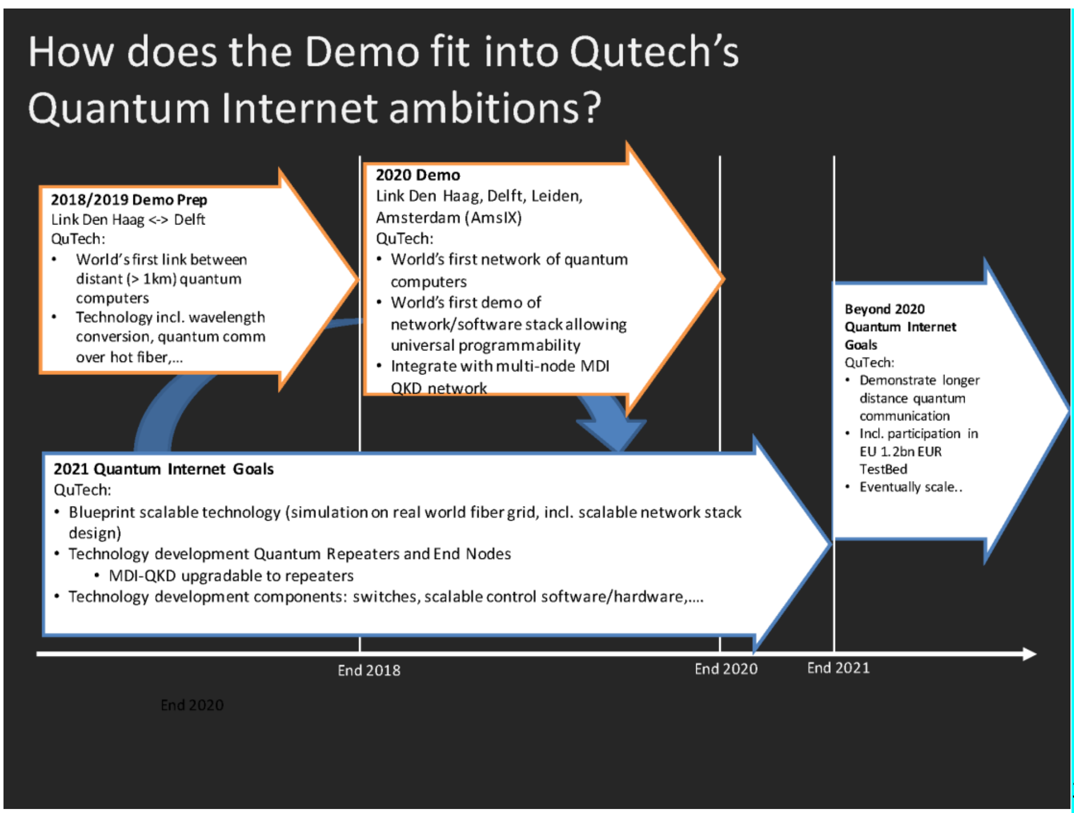


Figure 1: Computational complexity is defined by Turing machines (TM) providing digital models of computing [1, 62, 63]: deterministic TM (DTM); quantum TM (QTM); classical non-deterministic TM (NTM). Tractable problems are defined by polynomial time execution and define complexity classes: P denotes problems that are efficiently solvable with a classical computer; P is a subset of NP, the problems efficiently checkable by a classical computer. QMA denotes the problems efficiently checkable by a quantum computer. NP-hard problems are the problems at least as hard as any NP problem, and QMA-hard problems are the problems at least as hard as any QMA problem. For a nice tutorial on how to classify combinatorial problems, including games, see [61].


What's a quantum internet?
QC
QC
QC
GOAL: Communicate qubits between any two points on earth


Why construct a quantum internet?
For Quantum Communication
• Quantum secure communications
• Clock synchronization
• Combining telescopes
• Testing Physics
• Exponential savings in communication
• Cheating online games ☺
• ….
For Quantum Computation
• Linking small quantum computers
• Access the quantum "mainframe"



[31]

---

[31] Quantum Internet by QU Tech in the Netherlands

How much does a quantum computer cost?