Quantum Computing Standards and Why We Need Them

Presented to
The Chicago Quantum Computing MeetUp Group

November 25, 2018

William Favre Slater, III

M.S., MBA, PMP, CISSP, SSCP, CISA, ITIL v3

Cybersecurity Engineer, Adjunct Industry Professor, Writer, and Researcher in Blockchain and Quantum Science

Abstract

- Quantum Computing hardware and software is evolving rapidly and giving birth to a new paradigm in computing. But it requires an understanding of mathematical and quantum physics concepts that are unfamiliar to many who are used to computing with more traditional computing platforms and software. To enable this new paradigm of computing, industry leaders like the IEEE, Google, Microsoft, IBM, and Intel are working diligently to usher in this new era of computing. The Standards being formed by these thought leaders will help to accelerate the maturation, adoption, and use of quantum computing.

Agenda

- Where Are We Right Now In Traditional Computing?
- What is Quantum Computing?
- Quantum Computing Terminology
- Some Important Standards Around Computing and The Internet
- The Formation of Quantum Computing Standards
- The Potential and Promise of Quantum Computing
- Quantum Computing – The Downside
- How and Why Quantum Computing Will Persist, and Rapidly Evolve and Be Adopted
- A Cautionary Tale
- A Call to Action
- Conclusion
- References

Presentation Location

http://billslater.com/quantum/wslater_quantum01.pdf

Special Thanks to:

- Gene Naden – Founder & Leader of the Chicago Quantum MeetUp
- William Hurley – Quantum Computing researcher, writer, and Chair of the IEEE Quantum Standards Working Group

Gene Naden

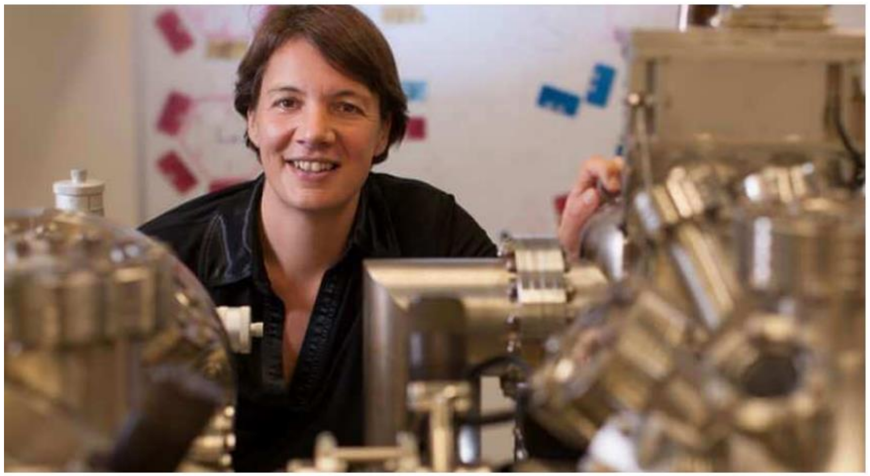
Programmer Extraordinaire
Mathematician
Astrophysicist
Quantum Computing Fan
Founder & Leader of
The Chicago Quantum Computing MeetUp
and
The Chicago Cosmology MeetUp

William Hurley a.k.a. whurley, founder and CEO of Strangeworks, and chair of the IEEE Quantum Standards Working Group

whurley is founder and CEO of Strangeworks, a quantum computing startup based in Austin, Texas. He is the Chair of the Quantum Standards Working Group at IEEE, and blogs about quantum computing on superposition.com. He has authored two books on the subject, Quantum Computing for Babies, a colorfully simple introduction to quantum computing and Endless Impossibilities, which brings the realities of a quantum future into the present, helping readers understand and prepare for the coming age of quantum computing.

Special Thanks to:

- Michelle Simmons – Working on the world's first quantum computer
- Urmila Mahadev – Worked eight years on the algorithm to prove a quantum computer performs its tasks



Woman Leads Team Looking To Build World's First Quantum Computer

Michelle Simmons

Fifty-year-old Michelle Simmons is on a mission to build the world's first quantum computer in Sydney.

Urmila Mahadev giving a computer science seminar last week at the University of California, Berkeley, ahead of her presentation yesterday at the Symposium on Foundations of Computer Science in Paris.


"The nicest thing about standards is that there are so many of them to choose from."
Ken Olsen

Where Are We Right Now in Computing? Top 500 List

Rank	System	Cores	Rmax (TFlop/s)	Rpeak (TFlop/s)	Power (kW)
1	**Summit** - IBM Power System AC922, IBM POWER9 22C 3.07GHz, NVIDIA Volta GV100, Dual-rail Mellanox EDR Infiniband , IBM DOE/SC/Oak Ridge National Laboratory United States	2,397,824	143,500.0	200,794.9	9,783
2	**Sierra** - IBM Power System S922LC, IBM POWER9 22C 3.1GHz, NVIDIA Volta GV100, Dual-rail Mellanox EDR Infiniband , IBM / NVIDIA / Mellanox DOE/NNSA/LLNL United States	1,572,480	94,640.0	125,712.0	7,438
3	**Sunway TaihuLight** - Sunway MPP, Sunway SW26010 260C 1.45GHz, Sunway , NRCPC National Supercomputing Center in Wuxi China	10,649,600	93,014.6	125,435.9	15,371
4	**Tianhe-2A** - TH-IVB-FEP Cluster, Intel Xeon E5-2692v2 12C 2.2GHz, TH Express-2, Matrix-2000 , NUDT National Super Computer Center in Guangzhou China	4,981,760	61,444.5	100,678.7	18,482
5	**Piz Daint** - Cray XC50, Xeon E5-2690v3 12C 2.6GHz, Aries interconnect , NVIDIA Tesla P100 , Cray Inc. Swiss National Supercomputing Centre (CSCS) Switzerland	387,872	21,230.0	27,154.3	2,384

Source: https://www.top500.org/lists/2018/11/

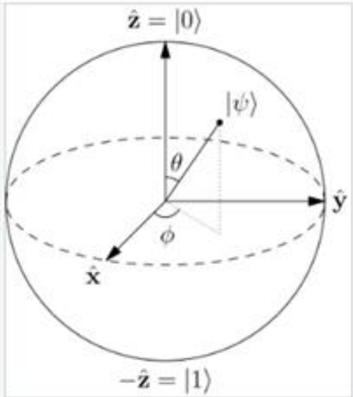
WHAT IS QUANTUM COMPUTING?

What is Quantum Computing?

Quantum computing is computing using quantum-mechanical phenomena, such as superposition and entanglement.[1] A **quantum computer** is a device that performs quantum computing. Such a computer is different from binary digital electronic computers based on transistors. Whereas common digital computing requires that the data be encoded into binary digits (bits), each of which is always in one of two definite states (0 or 1), quantum computation uses quantum bits or qubits, which can be in superpositions of states. A quantum Turing machine is a theoretical model of such a computer and is also known as the universal quantum computer. The field of quantum computing was initiated by the work of Paul Benioff[2] and Yuri Manin in 1980,[3] Richard Feynman in 1982,[4] and David Deutsch in 1985.[5]

As of 2018, the development of actual quantum computers is still in its infancy, but experiments have been carried out in which quantum computational operations were executed on a very small number of quantum bits.[6] Both practical and theoretical research continues, and many national governments and military agencies are funding quantum computing research in additional effort to develop quantum computers for civilian, business, trade, environmental and national security purposes, such as cryptanalysis.[7] A small 20-qubit quantum computer exists and is available for experiments via the IBM Quantum Experience project. D-Wave Systems has been developing their own version of a quantum computer that uses annealing.[8]

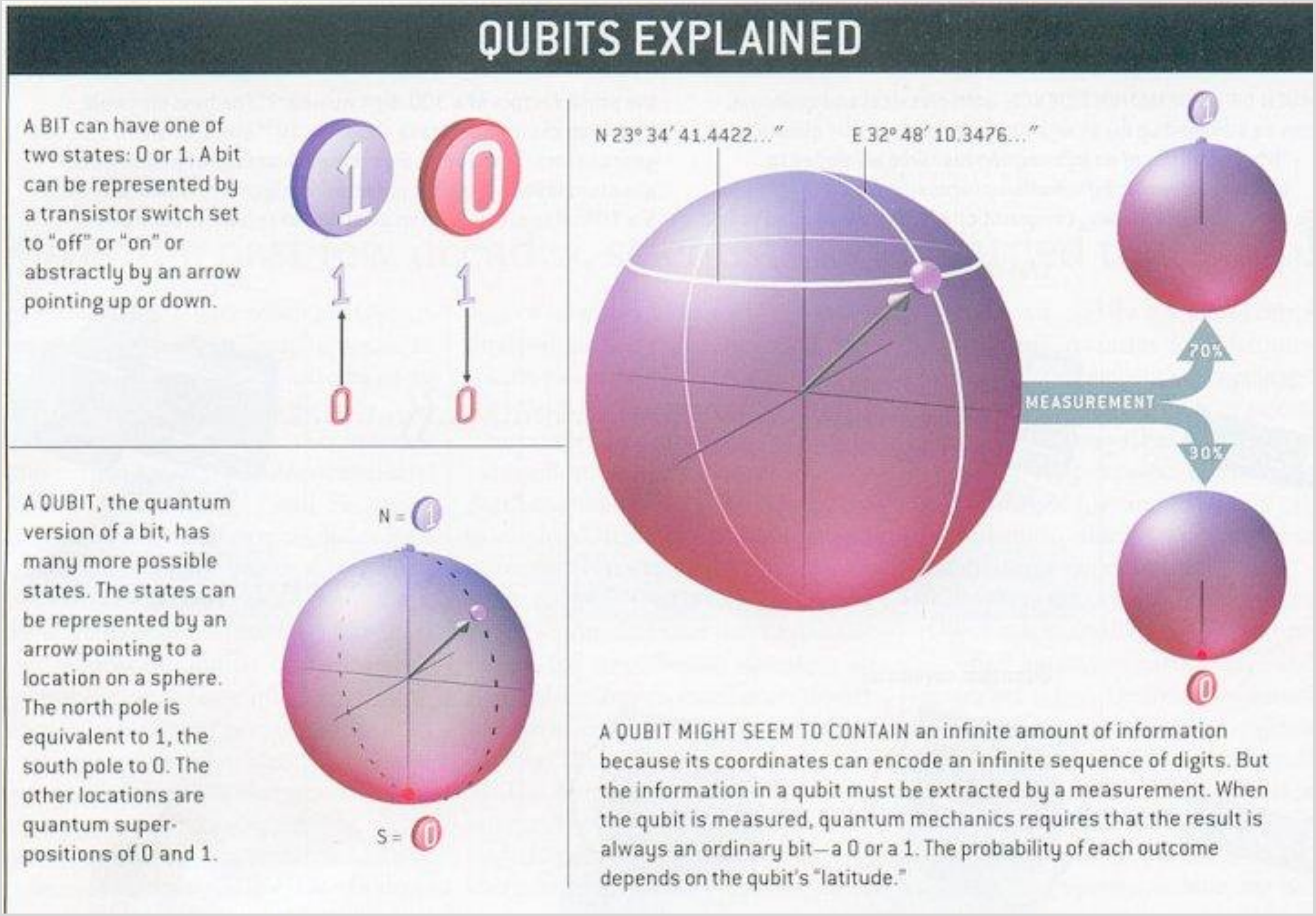
Large-scale quantum computers would theoretically be able to solve certain problems much more quickly than any classical computers that use even the best currently known algorithms, like integer factorization using Shor's algorithm (which is a quantum algorithm) and the simulation of quantum many-body systems. There exist quantum algorithms, such as Simon's algorithm, that run faster than any possible probabilistic classical algorithm.[9] A classical computer could in principle (with exponential resources) simulate a quantum algorithm, as quantum computation does not violate the Church–Turing thesis.[10]:202 On the other hand, quantum computers may be able to efficiently solve problems which are not *practically* feasible on classical computers.



The Bloch sphere is a representation of a qubit, the fundamental building block of quantum computers.

Source: Wikipedia. https://en.wikipedia.org/wiki/Quantum_computing

Qubits Explained



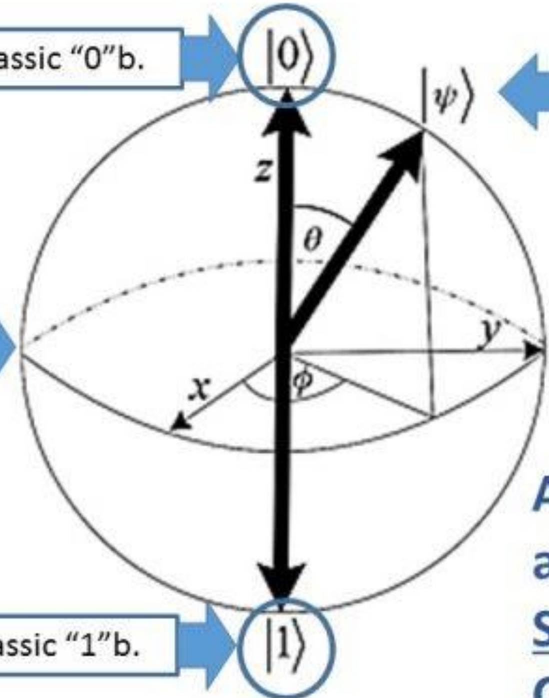
Source: Wikipedia. https://www.autodesk.com/products/eagle/blog/future-computing-quantum-qubits/

Qubits Explained

What If We Don't Limit Ourselves to 1's and 0's? The Quantum Computer Qubit

Here's your classic "0"b.

Note: Even though you cannot look inside the qubit and see it during quantum computation, all the points on the Bloch sphere are part of the quantum computation. When the computation is over, you'll read the qubit and see "0"b or "1"b but that doesn't happen until the end of the quantum operation.



Here's your classic "1"b.

A Quantum Qubit

$$|\psi\rangle = \begin{bmatrix} c_0 \\ c_1 \end{bmatrix}$$

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle$$

$$|\psi\rangle = cos(\theta)\,|0\rangle + ei^{\phi}\,sin(\Theta)\,|1\rangle$$

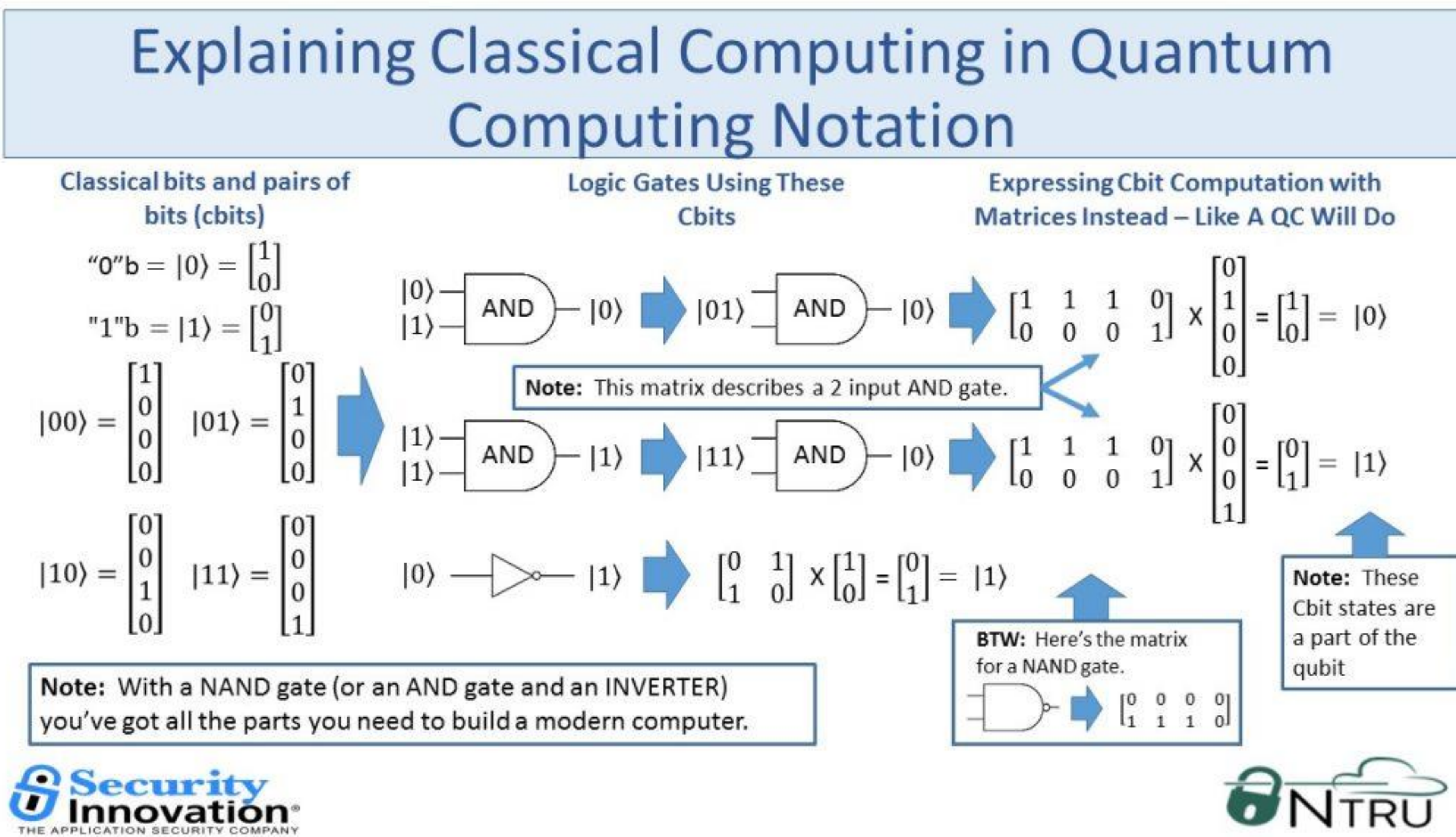
A Bloch Sphere Represents a Quantum Qubit – And It Still Uses the Traditional Cbit

Security Innovation – THE APPLICATION SECURITY COMPANY

NTRU

Source: Lee Wilson: http://www.activecyber.net/rise-quantum-computers-current-state-cryptographic-affairs/

Qubits Explained



Source: Lee Wilson: http://www.activecyber.net/rise-quantum-computers-current-state-cryptographic-affairs/

QUANTUM COMPUTING TERMINOLOGY

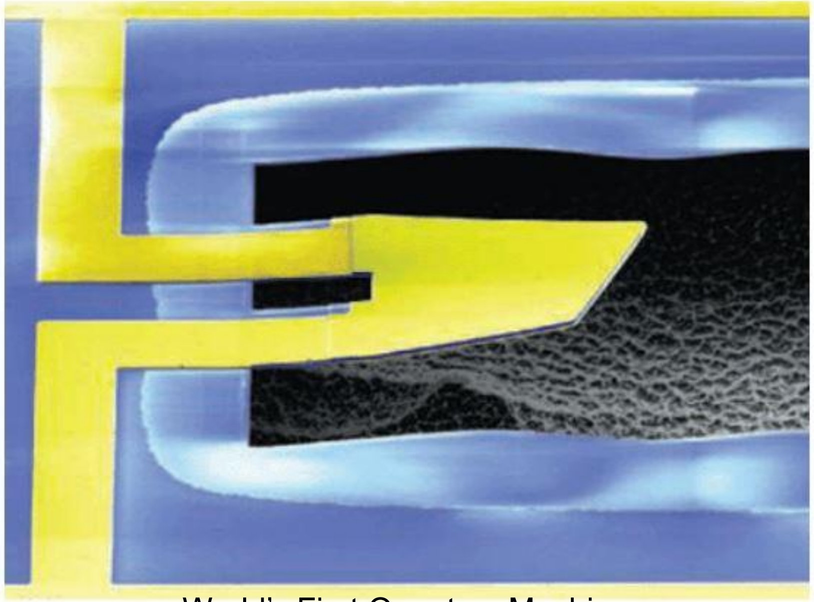
Quantum Computing Terminology

Absolute Zero — Absolute zero is the lowest temperature that is theoretically possible, at which the motion of particles that constitutes heat would be minimal. It is zero on the Kelvin scale, equivalent to –273.15°C or –459.67°F. In order to increase stability, most quantum computing systems operate at temperatures near absolute zero.

Algorithm — An algorithm is the specification of a precise set of instructions that can be mechanically applied to yield the solution to any given instance of a problem.

Anyon — An anyon is an elementary particle or particle-like excitation having properties intermediate between those of bosons and fermions. The anyon is sometimes referred to as a Majorana fermion but a more appropriate term to apply to the anyon is a particle in a Majorana bound state or in a Majorana zero mode. This name is more appropriate than Majorana fermion because the statistics of these objects is no longer fermionic. Instead, the Majorana bound states are an example of non-abelian anyons: interchanging them changes the state of the system in a way that depends only on the order in which the exchange was performed. The non-abelian statistics that Majorana bound states possess allows them to be used as a building block for a topological quantum computer.

Bose-Einstein Condensate — The Bose-Einstein Condensate is a super-cold cloud of atoms that behaves like a single atom that was predicted by Albert Einstein and Indian theorist Satyendra Nath Bose. Peter Engels, a researcher at Washington State University, explains, "This large group of atoms does not behave like a bunch of balls in a bucket. It behaves as one big super-atom. Therefore it magnifies the effects of quantum mechanics." Theoretically, a Bose-Einstein condensate (BEC) can act as a stable qubit.



World's First Quantum Machine

Bose-Einstein Condensate

Source: https://www.enterrasolutions.com/blog/glossary-quantum-computing-terms/

Quantum Computing Terminology

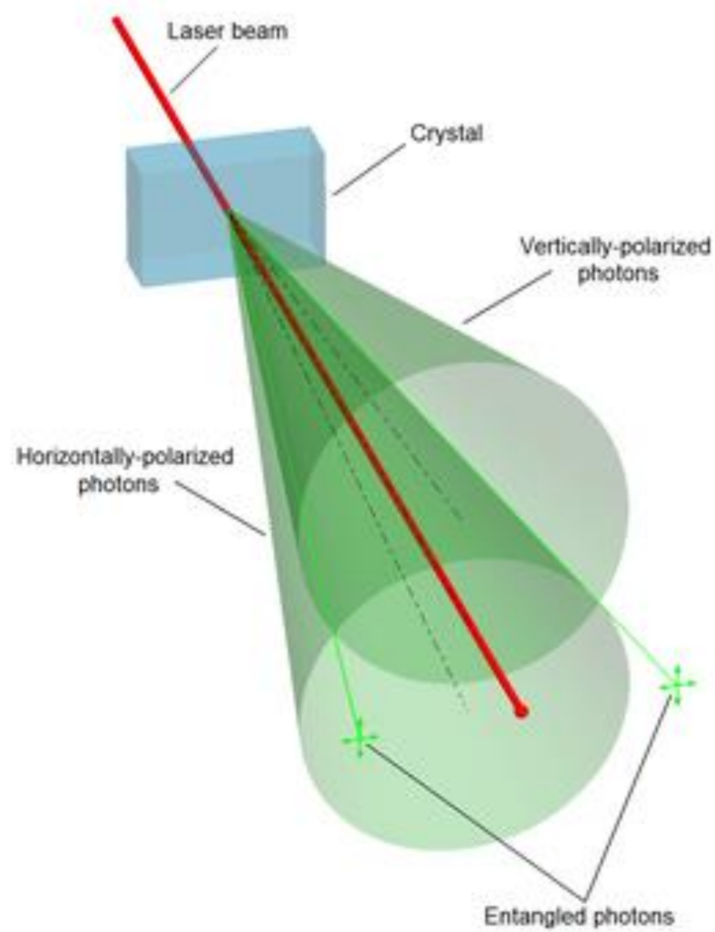
Coherence Time — Coherence time is the length of time a quantum superposition state can survive.

Doped Diamonds — A doped diamond is one into which a defect has been intentionally added. Physicists have discovered that they can can make good use of these defects to manipulating the spin of quantum particles.

Entanglement — Entanglement is a physical phenomenon that occurs when pairs or groups of particles are generated or interact in ways such that the quantum state of each particle cannot be described independently. If you think that is difficult to understand, you're not alone. Albert Einstein referred to this phenomenon as "spooky action at a distance."

'Fault-tolerant' Material —Fault tolerant materials are a unique class of advanced materials that are electrically insulating on the inside but conducting on the surface. Inducing high-temperature superconductivity on the surface of a topological insulator opens the door to the creation of a pre-requisite for fault-tolerant quantum computing. One of those materials is graphene. Interestingly, the edges of graphene basically turn it into a kind of topological insulator that could be used in quantum computers.

Magic State Distillation — Magic State Distillation is the "magic" behind universal quantum computation. It is a particular approach to building noise-resistant quantum computers. To overcome the detrimental effects of unwanted noise, so-called "fault-tolerant" techniques are developed and employed. Magic states are an essential (but difficult to achieve and maintain) extra ingredient that boosts the power of a quantum device to achieve the improved processing power of a quantum computer.



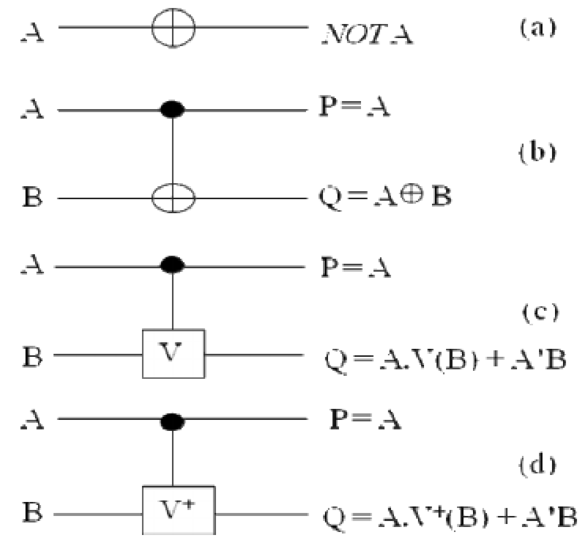
Source: https://www.enterrasolutions.com/blog/glossary-quantum-computing-terms/

Quantum Computing Terminology

Micro-drum — A micro-drum is a microscopic mechanical drum. It has been reported that physicists at the National Institute of Standards and Technology (NIST) have 'entangled' a microscopic mechanical drum with electrical signals confirming that it could be used as a quantum memory. NIST's achievement also marks the first-ever entanglement of a macroscopic oscillator which expands the range of practical uses of the drum.

Quantum Contextuality — Quantum contextuality is a phenomenon necessary for the "magic" behind universal quantum computation. Physicists have long known that measuring things at the quantum level establishes a state that didn't exist before the measurement. In other words, what you measure necessarily depends on how you carried out the observation – it depends on the 'context' of the experiment. Scientists at the Perimeter Institute for Theoretical Physics have discovered that this context is the key to unlocking the potential power of quantum computation.

Quantum Logic Gates — In quantum computing and specifically the quantum circuit model of computation, a quantum gate (or quantum logic gate) is a basic quantum circuit operating on a small number of qubits. They are the building blocks of quantum circuits, like classical logic gates are for conventional digital circuits. Quantum logic gates are represented by unitary matrices. The most common quantum gates operate on spaces of one or two qubits, just like the common classical logic gates operate on one or two bits. This means that as matrices, quantum gates can be described by 2 × 2 or 4 × 4 unitary matrices. Quantum gates are usually represented as matrices. A gate which acts on k qubits is represented by a 2k x 2k unitary matrix. The number of qubits in the input and output of the gate have to be equal.



Gate	Notation	Matrix
NOT (Pauli-X)	X	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Z	Z	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard	H	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
CNOT (Controlled NOT)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

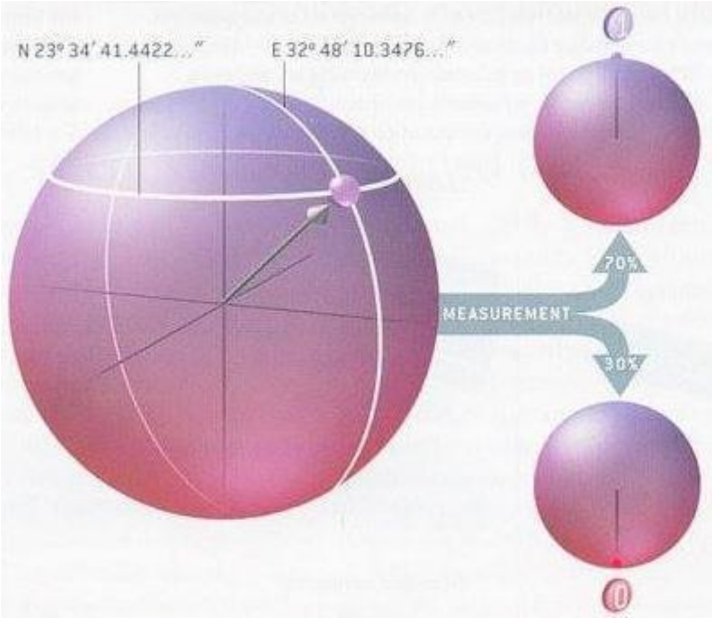
Source: https://www.enterrasolutions.com/blog/glossary-quantum-computing-terms/

Quantum Computing Terminology

Quantum Memory State — Quantum Memory State is the state in which qubits much sustain themselves in order to be of value in quantum computing. To date, these states have proved extremely fragile because the least bit of interference at the quantum level can destroy them. For this reason, most experiments with qubits require particles to be cooled to near absolute zero as well as heavy shielding.

Quantum Register — A collection of *n* qubits is called a *quantum register* of size *n*.

Qubit — A quantum bit or qubit operates in the weirdly wonderful world of quantum mechanics. At that level, subatomic particles can exist in multiple states at once. This is multi-state capability is called superposition. One commonly used particle is the electron, and state normally used to generate a superposition is spin (spin up could represent a "0" and spin down could represent a "1". Additional qubits can be added by a process called entanglement. Theoretically, each extra entangled qubit doubles the number of parallel operations that can be carried out. MIT's Seth Lloyd notes, "We could map the whole Universe — all of the information that has existed since the Big Bang — onto 300 qubits."

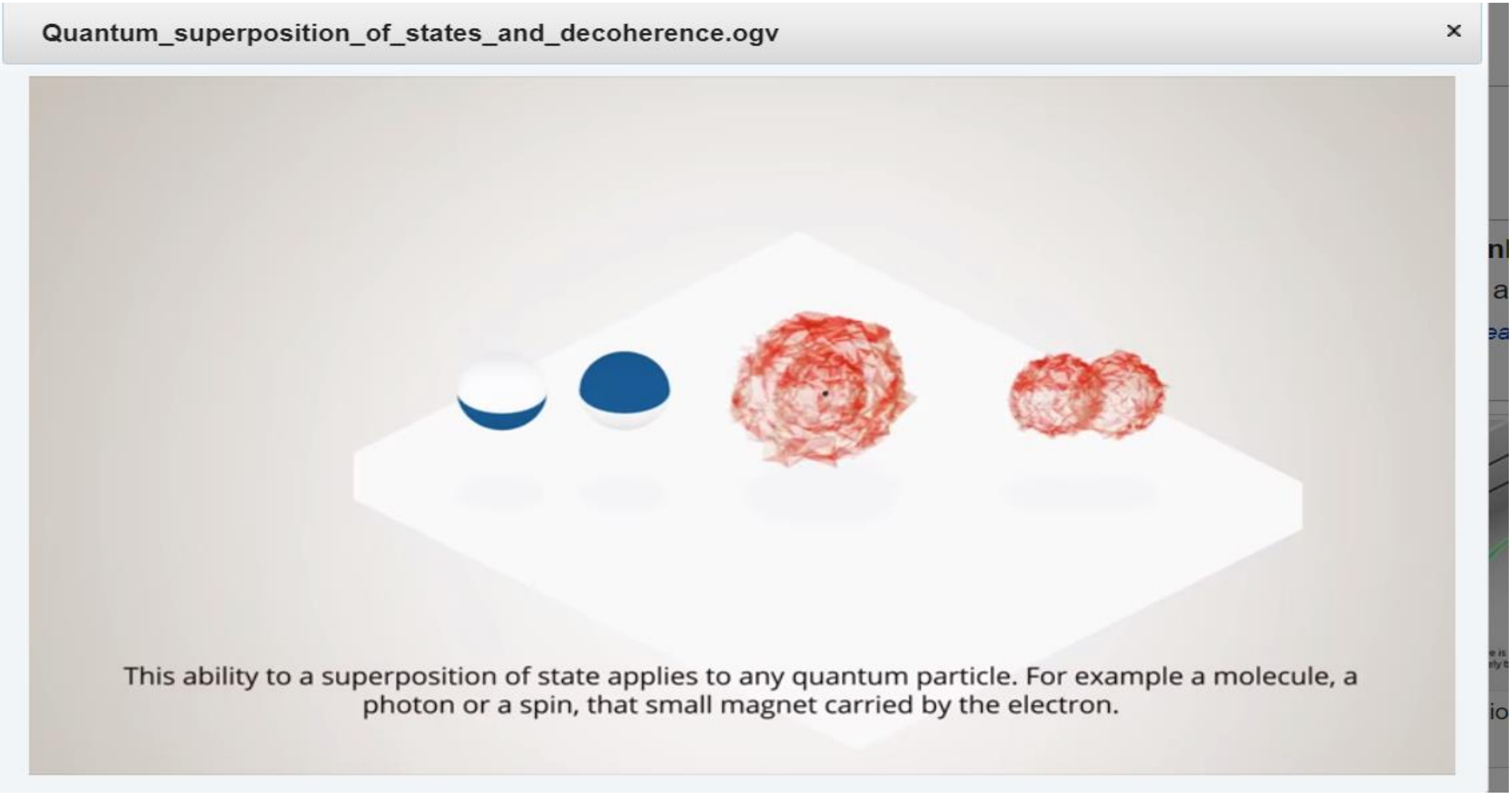


Spin — Spin sometimes called "nuclear spin" or "intrinsic spin" is the quantum version form of angular momentum carried by elementary particles, composite particles (hadrons), and atomic nuclei. Having said that, the website Ask a Mathematician/Ask a Physicist states, "Spin has nothing to do with actual spinning. … Physicists use the word 'spin' or 'intrinsic spin' to distinguish the angular momentum that particles 'just kinda have' from the regular angular momentum of physically rotating things."

Source: https://www.enterrasolutions.com/blog/glossary-quantum-computing-terms/

Quantum Computing Terminology

Superposition — Superposition is an ambiguous state in which a particle can be both a “0” and a “1”.



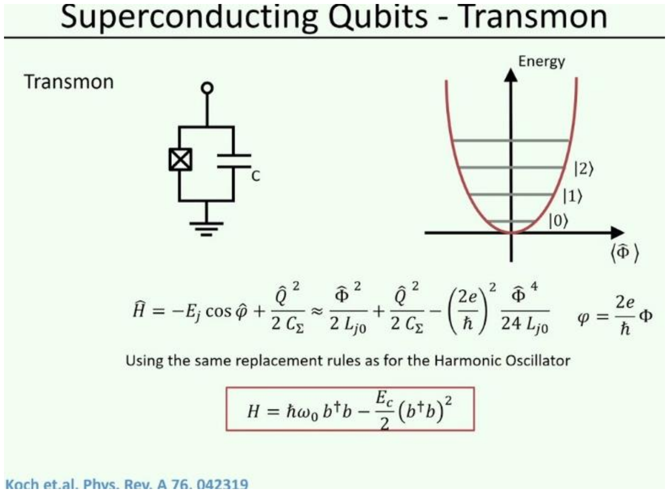
Source: https://www.enterrasolutions.com/blog/glossary-quantum-computing-terms/
and https://en.wikipedia.org/wiki/Quantum_superposition

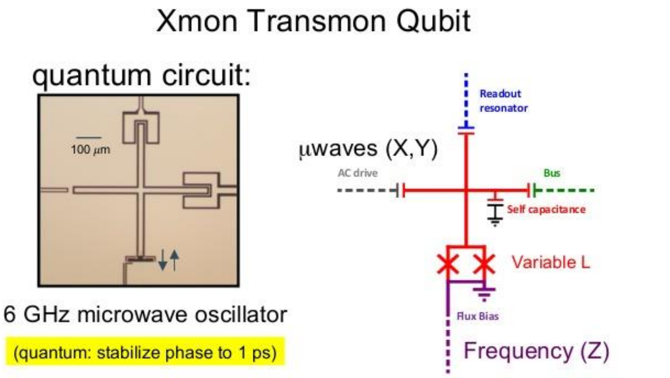
Quantum Computing Terminology

Topological Qubit — Topological qubits rely on a rare and extraordinarily finicky quantum state; however, once formed, they theoretically would behave like sturdy knots — resistant to the disturbances that wreck the delicate properties of every other kind of qubit.

Transmon — A transmon is a superconducting loop-shaped qubit that can be created at extremely low temperatures and, at the moment, up to five of them can be linked together. A standard transmon can maintain its coherence for around 50 microseconds – long enough to be used in quantum circuits. What's more, coherence times twice that length, and transmon arrays of 10 to 20 loops, are supposedly just around the corner.

Xmon — An Xmon is a cross-shaped qubit created by a team at the University of California, Santa Barbara. The team found that by placing five Xmons in a single row (with each qubit talking to its nearest neighbor) they were able to create a stable and effective quantum arrangement that provides the most stability and fewest errors. Like most other qubits, the Xmon must be created at temperatures approaching absolute zero.





Source: https://www.enterrasolutions.com/blog/glossary-quantum-computing-terms/

SOME IMPORTANT STANDARDS AROUND COMPUTING AND THE INTERNET

Some Important Standards Around Computing and The Internet

- **Free**
  - IETF's RFCs (TCP/IP, HTTP, SMTP, SNMP, IPv4, NAT, ARP, BGMP IPv6, MIBs, etc.)
  - NIST (NIST SP 800 Series, NIST Cybersecurity Framework, etc.)
  - W3C – (HTML 4.0, HTML 5.0, XML, etc.)
  - OMG – (CORBA, UML, etc.)
  - Open Source
- **Not Free**
  - ISO Standards (i.e. ISO 2700x, ISO 20000, ISO 19011, ISO 9001 etc.)
  - IEEE (i.e. 802.3 (Ethernet), 802.11x (Wireless), etc.)
  - ANSI

THE FORMATION OF QUANTUM COMPUTING STANDARDS

The Formation of Quantum Computing Standards

- Slides 25 – 40 (except slide 28) are from William Hurley (@whurley) Chairman of the IEEE Quantum Computing Standards Working Group. Delivered in a Webinar on April 24, 2018.

William Hurley a.k.a. whurley, founder and CEO of Strangeworks, and chair of the IEEE Quantum Standards Working Group

whurley is founder and CEO of Strangeworks, a quantum computing startup based in Austin, Texas. He is the Chair of the Quantum Standards Working Group at IEEE, and blogs about quantum computing on superposition.com. He has authored two books on the subject, Quantum Computing for Babies, a colorfully simple introduction to quantum computing and Endless Impossibilities, which brings the realities of a quantum future into the present, helping readers understand and prepare for the coming age of quantum computing.

Agenda: Quantum Computing Standards

A few of the things we will cover before the Q&A

- High-level overview
  - Quantum Computing 101
- Current state of industry
  - Nascent, fractured, in need of standards
- Challenges faced by industry
  - Multiple technical approaches
  - Lack of standards
- IEEE's proposed solutions
  - IEEE P7130™
  - IEEE P7131™
- Who is involved
- How to get involved

3

IEEE

Source: William Hurley (@whurley) Chairman of the IEEE Quantum Computing Standards Working Group. Delivered in a webinar on April 24, 2018. https://www.youtube.com/watch?v=qKt7dOf4pXY&t=7s

Quantum Computing 101

An extremely high level overview

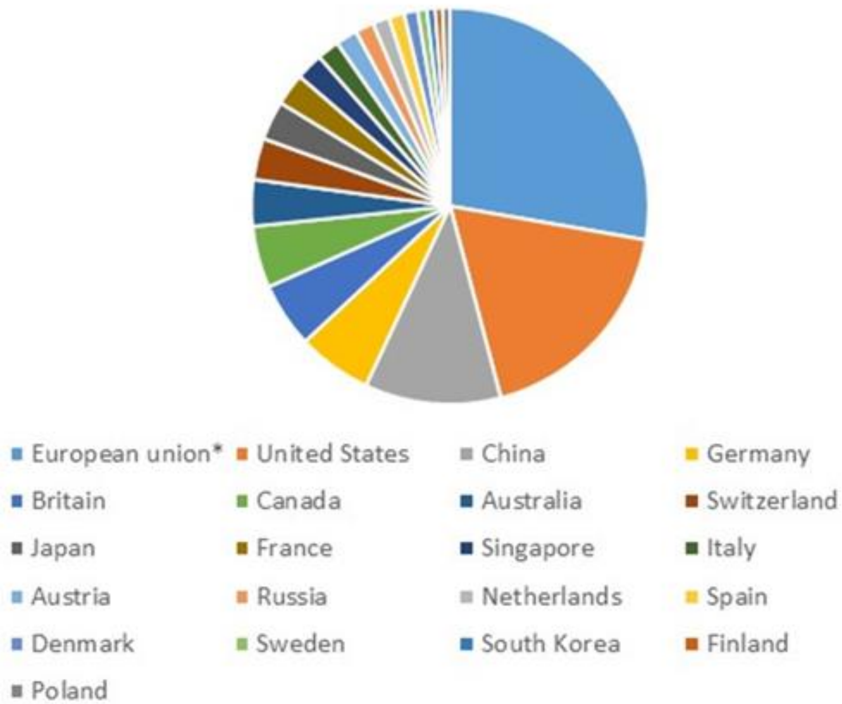
> Speaking: whurley

- Takes advantage of quantum mechanics
  - Superposition
  - Entanglement
- Should be approached as a co-processor / cloud processor
  - Not a replacement for classical computers. In fact dependent on classical computers to operate.

Source: William Hurley (@whurley) Chairman of the IEEE Quantum Computing Standards Working Group. Delivered in a webinar on April 24, 2018. https://www.youtube.com/watch?v=qKt7dOf4pXY&t=7s

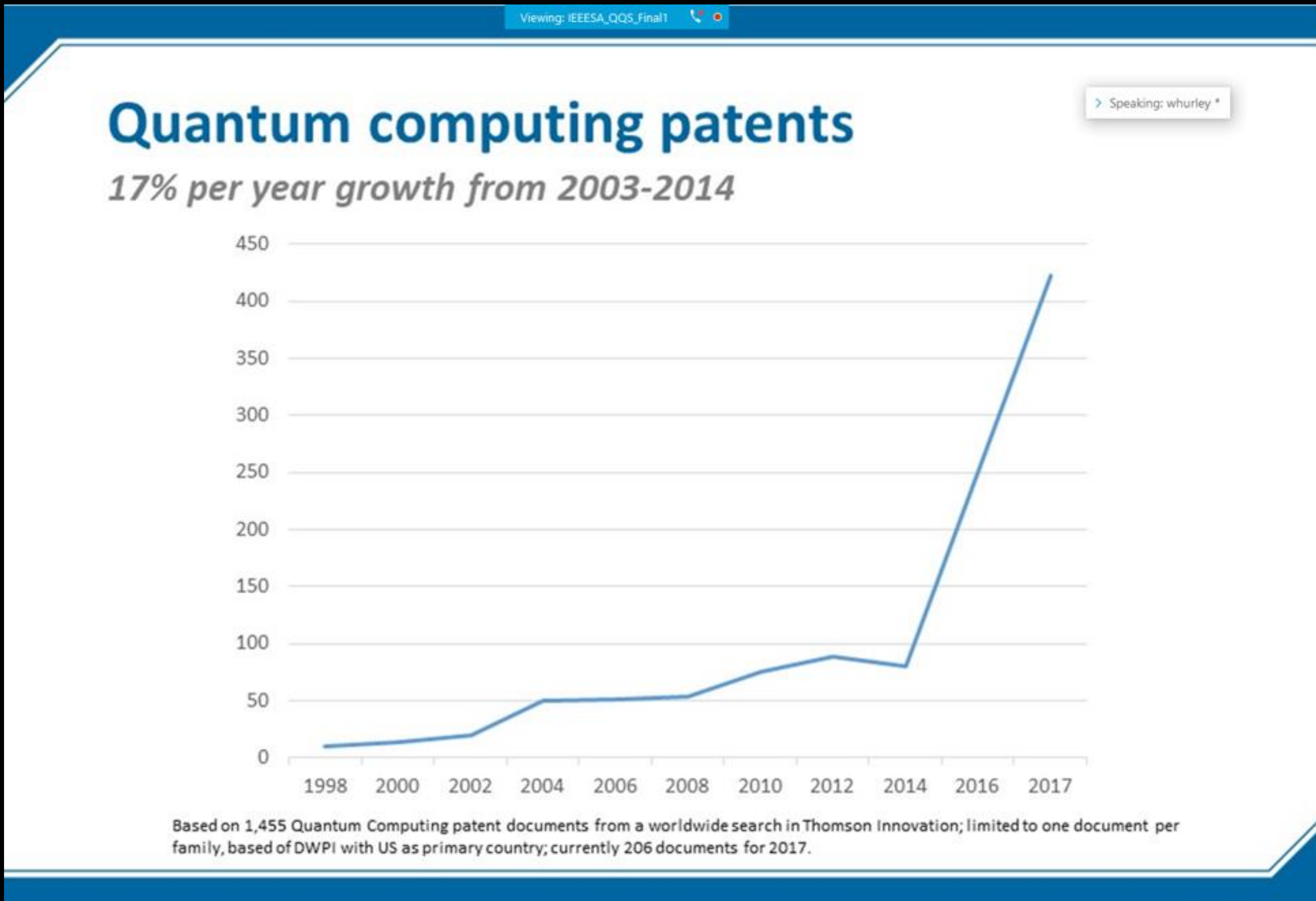
Investment in Quantum Computing

Estimated annual spending on non-classified quantum-technology research, 2015, €m



Source: McKinsey
*Combined estimated budget for EU countries

Source: William Hurley (@whurley) Chairman of the IEEE Quantum Computing Standards Working Group. Delivered in a webinar on April 24, 2018. https://www.youtube.com/watch?v=qKt7dOf4pXY&t=7s



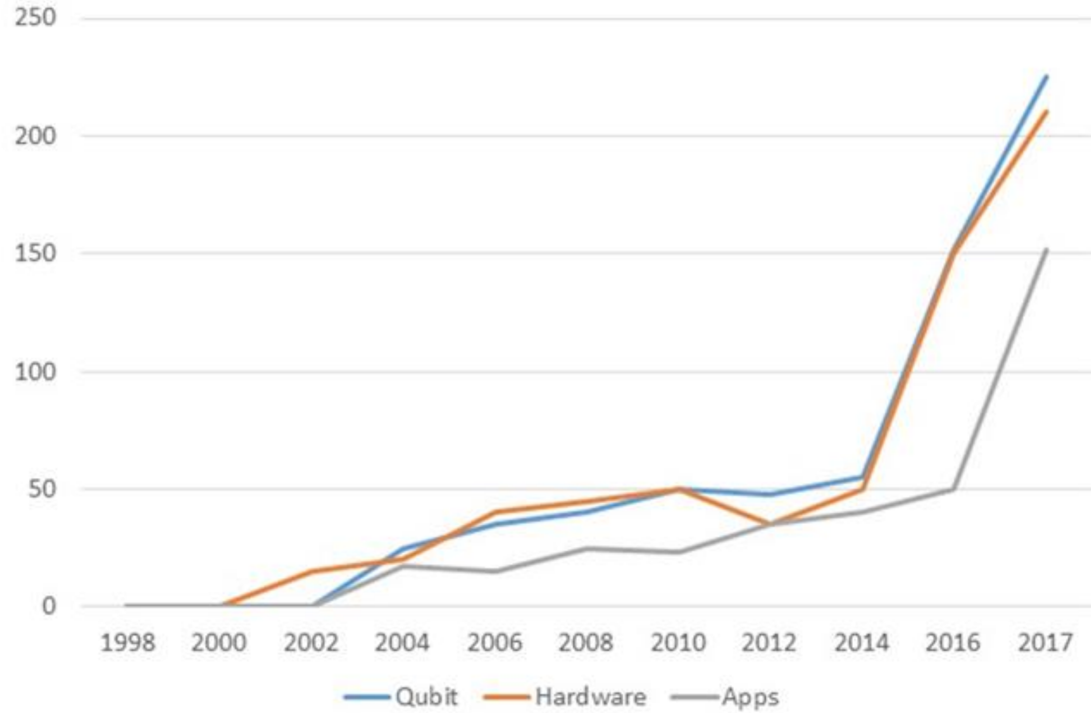
Source: William Hurley (@whurley) Chairman of the IEEE Quantum Computing Standards Working Group. Delivered in a webinar on April 24, 2018. https://www.youtube.com/watch?v=qKt7dOf4pXY&t=7s

Viewing: IEEESA_QQS_Final1

Speaking: whurley

Quantum computing patents (by family)

Publications related to qubit technology have the greatest amount of growth



Based on 1,952 Quantum Computing patent documents from a worldwide search in Thomson Innovation; limited to one document per family, based of DWPI with US as primary country; documents can appear in more than one category; currently 293 documents for 2017.

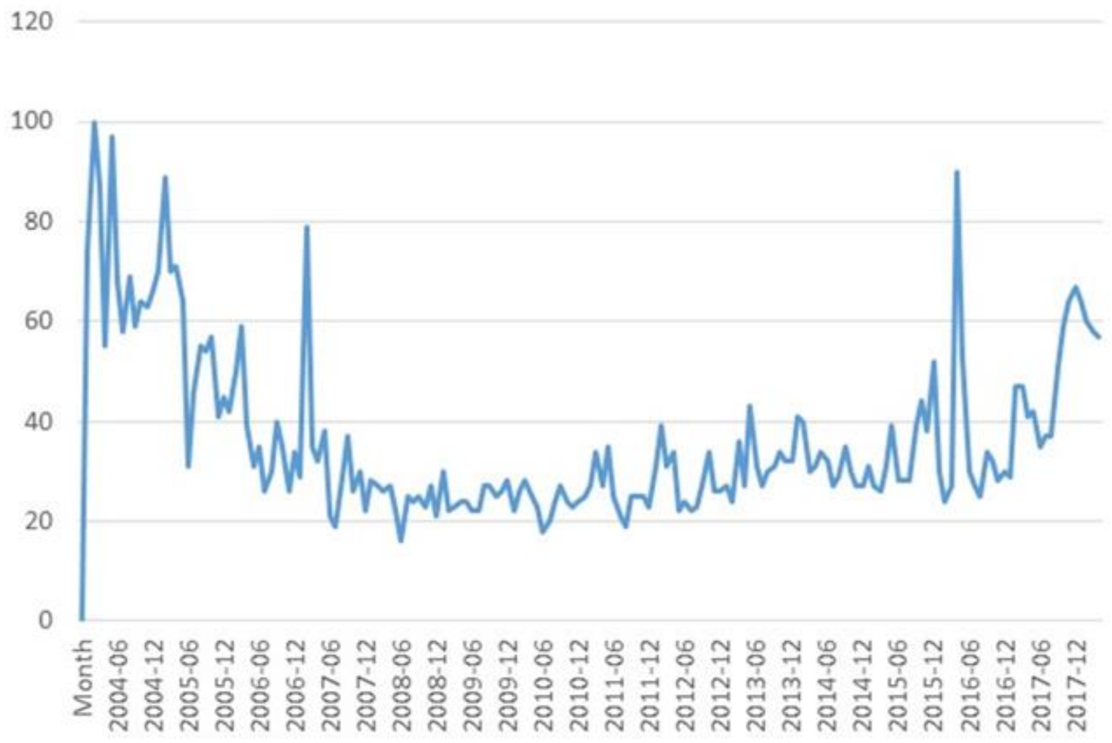
Source: William Hurley (@whurley) Chairman of the IEEE Quantum Computing Standards Working Group. Delivered in a webinar on April 24, 2018. https://www.youtube.com/watch?v=qKt7dOf4pXY&t=7s

Viewing: IEEESA_QQS_Final1

Speaking: whurley *

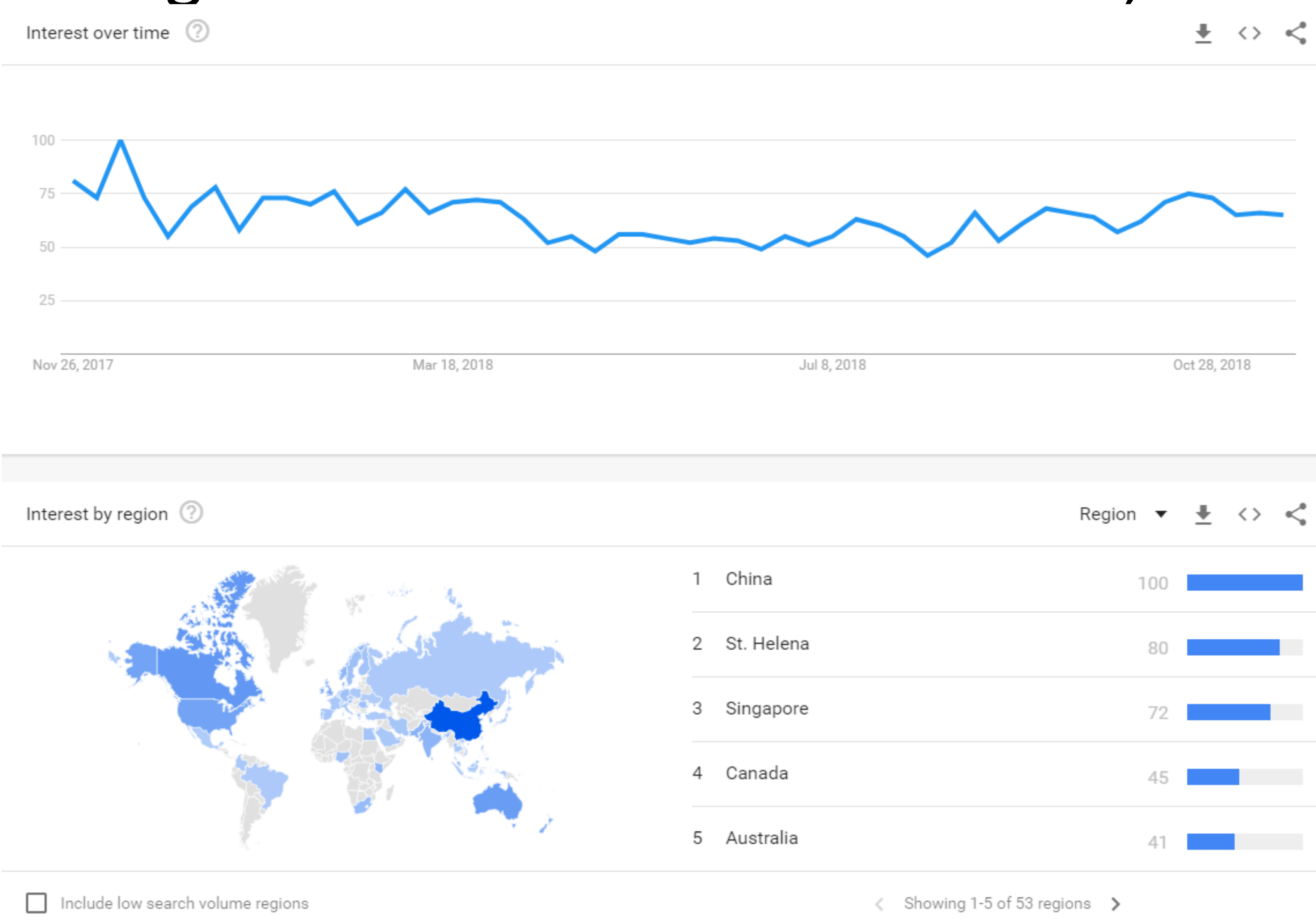
Google Trends

Quantum Computing: (Worldwide)



Source: William Hurley (@whurley) Chairman of the IEEE Quantum Computing Standards Working Group. Delivered in a webinar on April 24, 2018. https://www.youtube.com/watch?v=qKt7dOf4pXY&t=7s

Quantum Computing in Google Trends as of November 21, 2018



Viewing: IEEESA_QQS_Final1

Expand to view video

Current Industry Challenges

It's a mess!

- Definitions of quantum computers, qubits, and other key points vary widely creating confusion among researchers, engineers, investors, and potential buyers.
  - There are very different approaches to building one, so what exactly is a quantum computer?
    - Annealing (D•Wave)
    - Circuit gate (IBM, Google, Rigetti)
    - Topological (Microsoft)
  - We can't really define what a qubit is or how to count them
    - D•Wave has 2048 "Qubits"
    - IBM has 50 "Qubits"
    - Google has 72 "Qubits"
    - Microsoft has a qubit so powerful one of them is comparable to potentially hundreds of thousands or even millions of those other "Qubits"

Source: William Hurley (@whurley) Chairman of the IEEE Quantum Computing Standards Working Group. Delivered in a webinar on April 24, 2018. https://www.youtube.com/watch?v=qKt7dOf4pXY&t=7s

Viewing: IEEESA_QQS_Final1

Speaking: whurley

Current Industry Challenges

Various technical approaches cause confusion.

- Vendors:
  - "Obviously [Annealing, Circuit Gate Modeling, Topology] is the best architecture for quantum computing."
- Researchers:
  - "Well, I mean if you don't want to use ion traps or optical tweezers, duh."
- Investors:
  - "Yeah, call us back when...well anything."

Source: William Hurley (@whurley) Chairman of the IEEE Quantum Computing Standards Working Group. Delivered in a webinar on April 24, 2018. https://www.youtube.com/watch?v=qKt7dOf4pXY&t=7s

Viewing: IEEESA_QQS_Final1

Speaking: whurley

Current Industry Challenges

Benchmarking pretty much doesn't exist or can be easily debunked.

- Vendors:
  - "Our new quantum computer is a gazillion times faster than your classical computer… at something… we think."
- Researchers:
  - "No it's not, and here's the math to prove it."
- Investors:
  - "Yeah I'll just sit this out for a bit longer."

Source: William Hurley (@whurley) Chairman of the IEEE Quantum Computing Standards Working Group. Delivered in a webinar on April 24, 2018. https://www.youtube.com/watch?v=qKt7dOf4pXY&t=7s

Speaking: whurley

Current Industry Challenges

Consumers aren't participating because of lack of definition /understanding.

- Consumers:

Source: William Hurley (@whurley) Chairman of the IEEE Quantum Computing Standards Working Group. Delivered in a webinar on April 24, 2018. https://www.youtube.com/watch?v=qKt7dOf4pXY&t=7s

Viewing: IEEESA_QQS_Final1

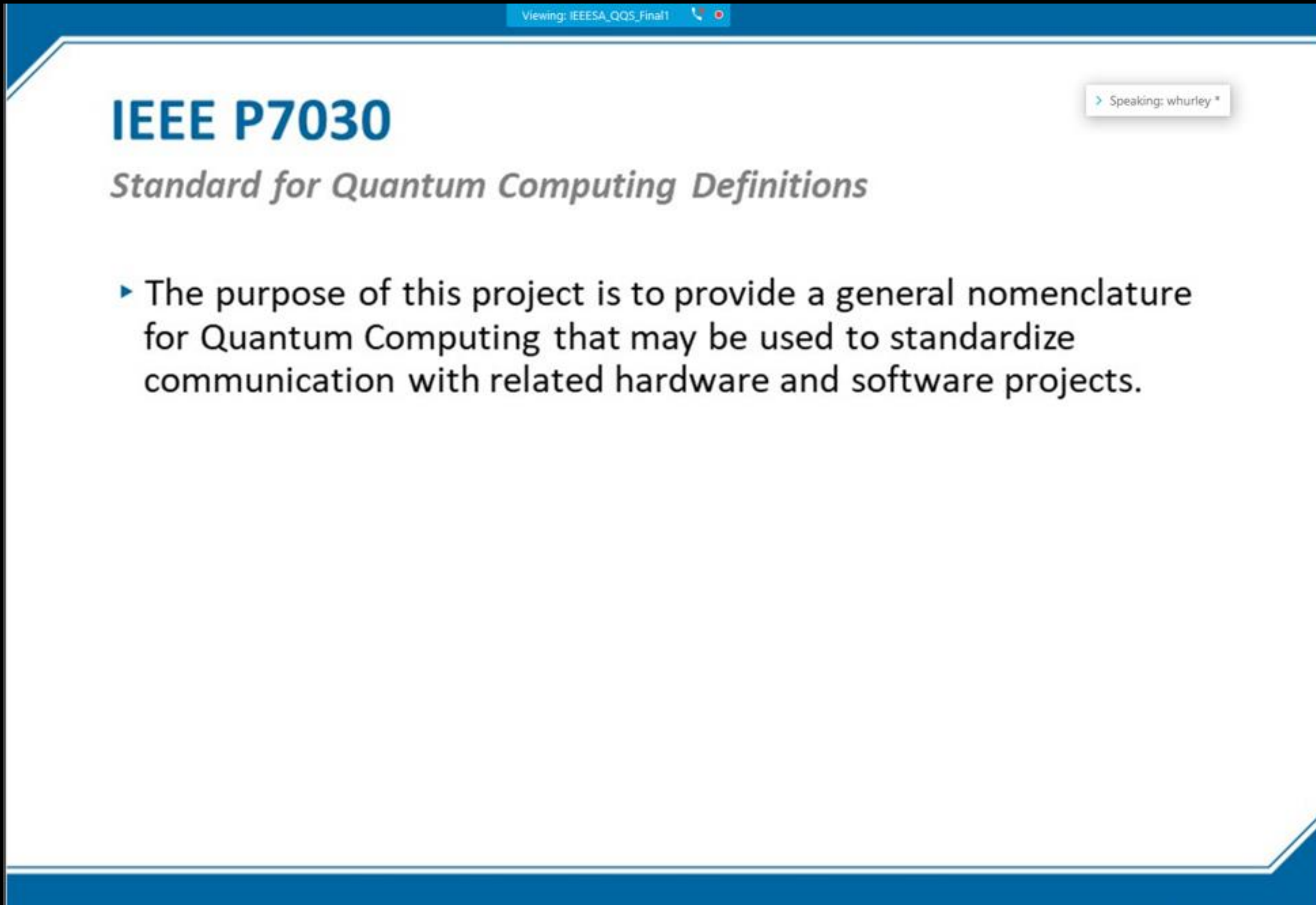
Speaking: whurley

IEEE Nomenclature Standard

How we're working to address the challenges of definition.

- IEEE P7130:
  - Standard for Quantum Computing Definitions
    - Working Group: QCWG - Quantum Computing Working Group
    - Sponsor: BOG/CAG - Corporate Advisory Group
    - Society: BOG - IEEE-SA Board of Governors
- For more information visit:
  - https://standards.ieee.org/develop/project/7130.html

Source: William Hurley (@whurley) Chairman of the IEEE Quantum Computing Standards Working Group. Delivered in a webinar on April 24, 2018. https://www.youtube.com/watch?v=qKt7dOf4pXY&t=7s



Source: William Hurley (@whurley) Chairman of the IEEE Quantum Computing Standards Working Group. Delivered in a webinar on April 24, 2018. https://www.youtube.com/watch?v=qKt7dOf4pXY&t=7s

IEEE Benchmarking Standard

How we're working to address the challenges of benchmarking.

- IEEE P7131:
  - Standard for Quantum Computing Performance Metrics & Performance Benchmarking
    - Working Group: QCWG - Quantum Computing Working Group
    - Sponsor: BOG/CAG - Corporate Advisory Group
    - Society: BOG - IEEE-SA Board of Governors
- For more information visit:
  - http://standards.ieee.org/develop/project/7131.html

Source: William Hurley (@whurley) Chairman of the IEEE Quantum Computing Standards Working Group. Delivered in a webinar on April 24, 2018. https://www.youtube.com/watch?v=qKt7dOf4pXY&t=7s

Source: William Hurley (@whurley) Chairman of the IEEE Quantum Computing Standards Working Group. Delivered in a webinar on April 24, 2018. https://www.youtube.com/watch?v=qKt7dOf4pXY&t=7s

Viewing: IEEESA_QQS_Final1

Speaking: whurley

How You Can Get Involved

WE want your help.

- Requires Corporate Participation
  - Your company must participate.
  - You can represent your company once approved.

- For more information email:
  - whurley@ieee.org

Source: William Hurley (@whurley) Chairman of the IEEE Quantum Computing Standards Working Group. Delivered in a webinar on April 24, 2018. https://www.youtube.com/watch?v=qKt7dOf4pXY&t=7s

THE POTENTIAL AND PROMISE OF QUANTUM COMPUTING

The Potential and Promise of Quantum Computing

Add more qubits and the quantum computing power actually grows exponentially—i.e. reading every book in the library at once happens faster and faster. So while conventional computers rely on huge numbers of transistors to achieve their computing speed, quantum computers use atoms and subatomic particles as their physical system. No one can predict where the particles will end up, or what form they will eventually take. As MIT physicist Seth Lloyd put it to *Wired* magazine, "Quantum mechanics is just counterintuitive and we just have to suck it up."[4]

But the numbers work, as do the computations. For example, Google and NASA are currently using a quantum computing machine (the D-WaveX2) that can do certain computations at one hundred million times the speed of a traditional computer chip—and that operates 3,600 times faster than the world's fastest digital supercomputer.

There are, in fact, three types of quantum computers currently in use. The D-Wave system is an example of a quantum annealer and is used for solving sampling and optimization problems, such as finding the best route between two points—something classical computers have great difficulty doing. Quantum annealers do not try to manipulate the qubits while they are computing, and therefore they can do calculations using one thousand qubits, which become entangled (able to exhibit multiple states) more or less at random.

The second type of quantum computing model is that of an analog emulator, which can simulate physical processes. This might include, for example, simulating certain aspects of the earth's climate in a controlled experiment or simulating the best way for electricity to be transmitted without loss. These simulators have been built with up to fifty-one qubits.

A universal quantum computer—the Holy Grail of quantum computing (and what most commentators are referring to when they discuss quantum computing)—would be able to run any type of algorithm and discover patterns in data sets that existing computers cannot analyze. The computing power needed for a universal quantum computer, however, requires entangling the qubits throughout the entire time of computing—a very difficult feat. At the moment, only twenty qubits have been effectively entangled in such a quantum computer.

Source: https://americanaffairsjournal.org/2018/05/winning-the-race-in-quantum-computing/

The Potential and Promise of Quantum Computing

Why is getting to the universal computer standard so difficult? Since subatomic particles are inherently unstable, keeping sufficient numbers of qubits entangled long enough to do calculations takes persistence, time, and resources.

The instability of qubits is called decoherence, and it is one of the chief engineering problems facing quantum scientists. When a qubit decoheres, it loses its superposition and can no longer act as both zero and one at the same time, but only one or the other, thus losing the ability to compute in a quantum manner. A qubit can decohere due to the slightest disturbance, which is why engineers are working on ways to mitigate the effects of minute disruptions of light, sound, and movement—and also why many quantum computers are built inside vacuums.

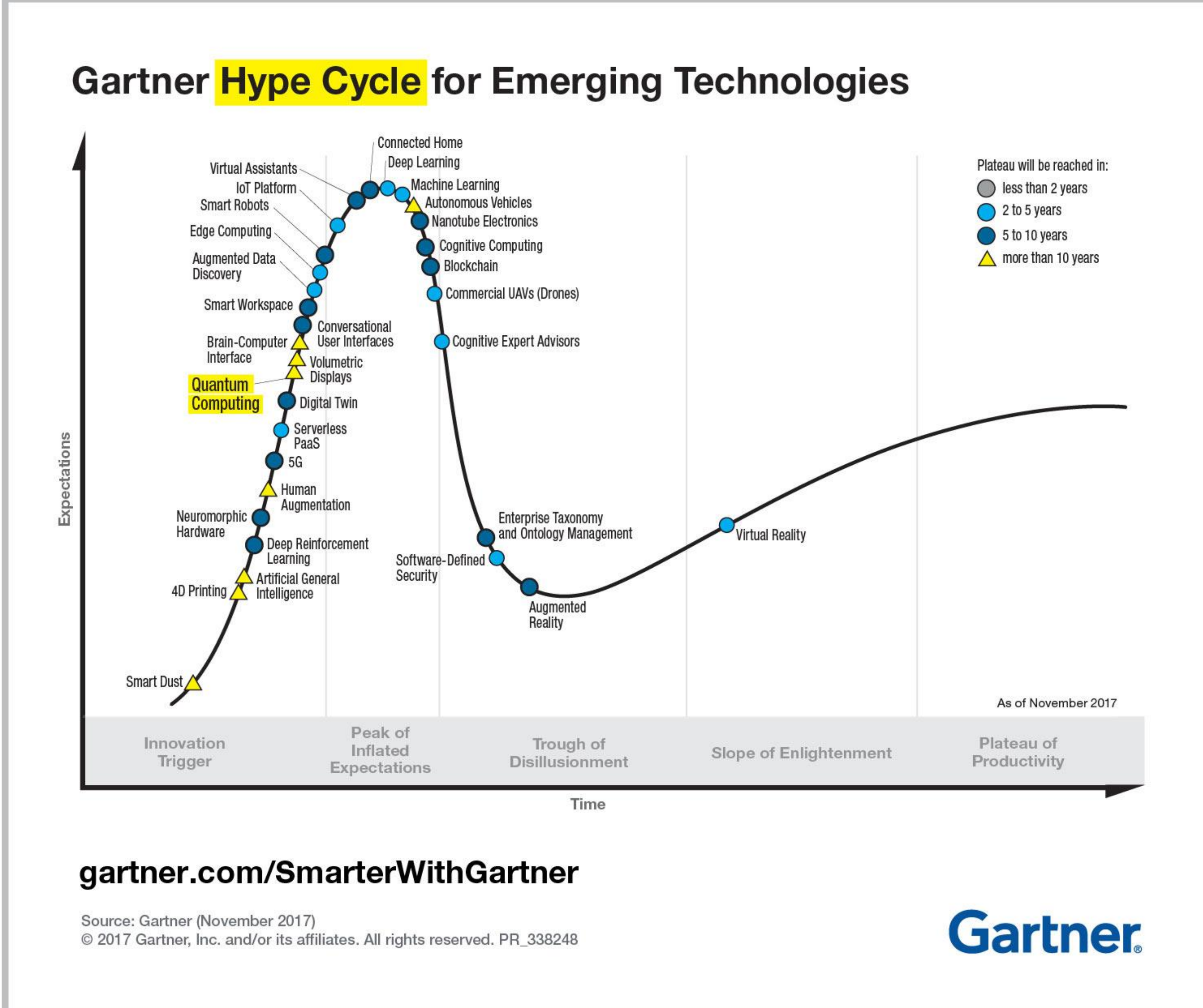
Nonetheless, a quantum computer capable of solving problems that would stump a classical computer is close at hand. Experts believe fifty qubits will be the formal threshold of "quantum supremacy." IBM recently claimed that its quantum computer had crossed the fifty-qubit threshold, but only for a few nanoseconds.[5] A breakthrough to genuine quantum supremacy is now a matter of applied engineering rather than scientific research—and only a matter of time.

Most experts agree that quantum computers will never completely displace conventional digital computers. Yet they will be deployed in an increasingly wide range of research activities and other complex tasks, bringing enormous improvements in performance and efficiency to areas such as weather forecasting, medical and genetic research, and tasks such as calculating traffic flows in the world's biggest cities—a task that D-Wave, a Canadian company, has already undertaken for China's capital Beijing.

And there is one thing quantum computers will be able to do that conventional computers cannot: hack conventional encryption systems around the world.

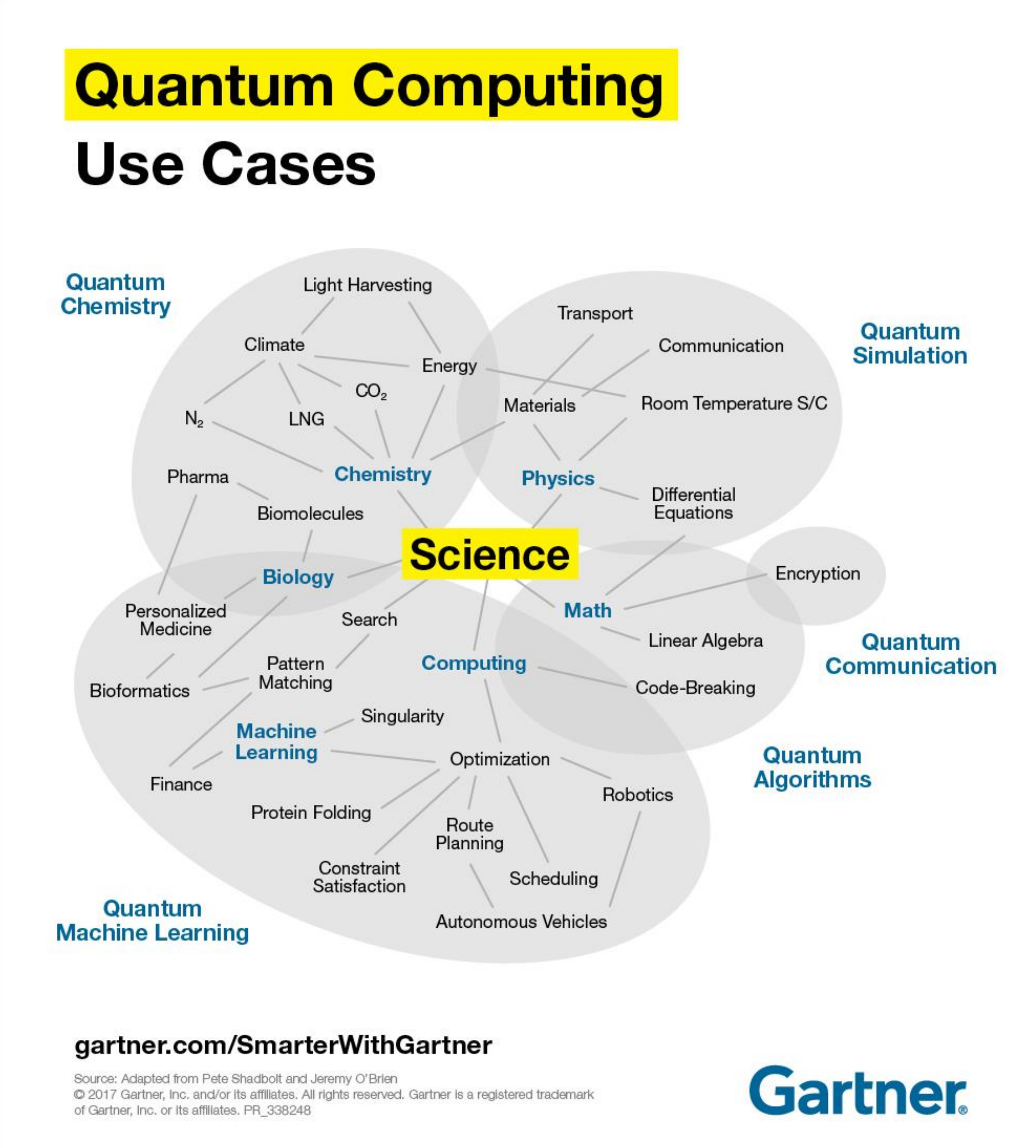
Source: https://americanaffairsjournal.org/2018/05/winning-the-race-in-quantum-computing/

The Potential and Promise of Quantum Computing



Source: https://www.gartner.com/smarterwithgartner/the-cios-guide-to-quantum-computing/

The Potential and Promise of Quantum Computing

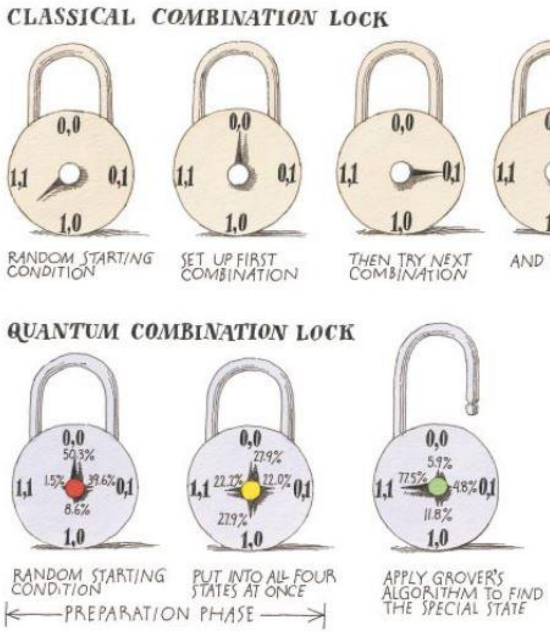


Source: https://www.gartner.com/smarterwithgartner/the-cios-guide-to-quantum-computing/

QUANTUM COMPUTING – THE DOWNSIDE

Quantum Computing – The Downside

- Huge shortage of talented people to do quantum-related work
- A real threat to encryption because Quantum Computing allows easy implementation of multiple proven algorithms
  - Shor
  - Grover
  - GEECM
- A real threat to Blockchain because of its ability to break encryption and hashes
- Unintended consequences because it will permit humans to find the answers to questions that were never imagined or even possible in traditional Von Neumann computing



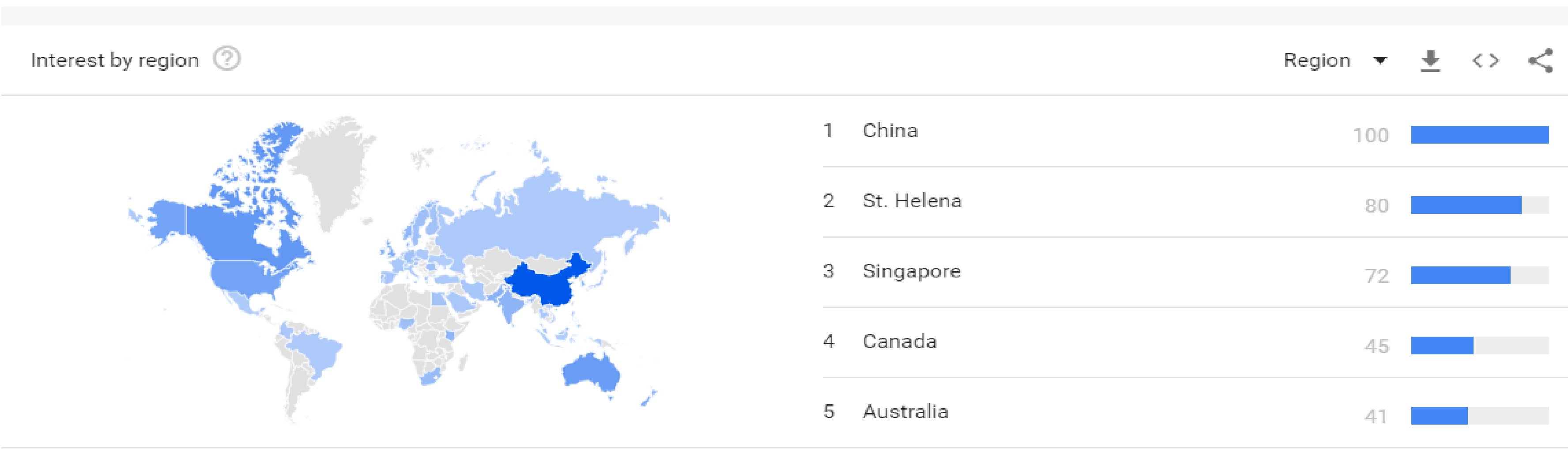
CRACKING A COMBINATION lock requires fewer tries with some quantum wizardry. For example, a two-bit classical lock might demand as many as four attempts to open it (*top*). On average, an *n*-bit lock requires about $^{n}/_{2}$ tries. Because a quantum lock can be put into multiple states at once, it takes only about $\sqrt{n}$ steps to open it if Grover's algorithm is used. The authors' experiment corresponds to opening a two-bit quantum lock, which (after suitable preparation) can be set to the right combination in a single step (*bottom*). The numbers shown on the dial indicate the relative populations measured for each of the four quantum states.

Source: http://cba.mit.edu/docs/papers/98.06.sciqc.pdf

HOW AND WHY QUANTUM COMPUTING WILL PERSIST, AND RAPIDLY EVOLVE AND BE ADOPTED

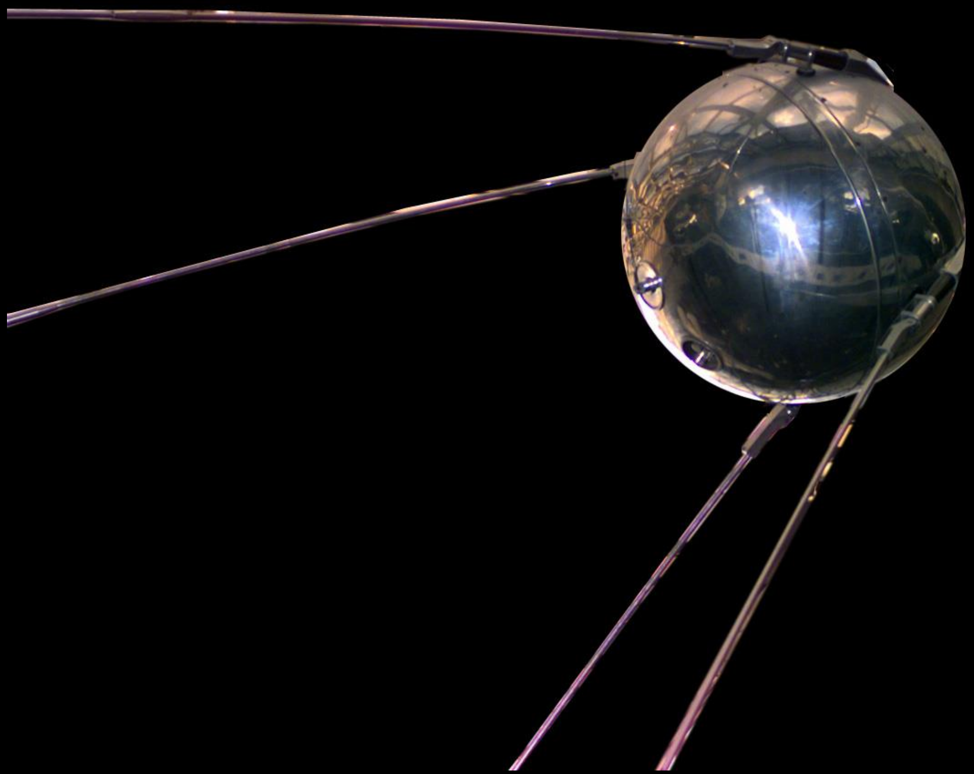
How and Why Quantum Computing Will Persist, and Rapidly Evolve and Be Adopted

- Standards will drive the maturation, adoption, and widespread use of quantum computers and quantum computing
- The power of quantum computing to solve big and complex problems much faster than their Von Neumann counterparts will make them more in demand.
- We are actually in a Quantum Science and Technology “Arms Race” with the Chinese, and by many accounts, they are winning.
- DARPA has several Quantum Computing projects, including Quiness and QuASAR.



Google Trends Result on “Quantum Computing” on November 21, 2018

And Still… America Needs a "***Sputnik Moment***" to Kick Us in Our Butts & Help Propel Our Progress in Quantum Science and Technology



A reference to the Soviet Union's 1957 launch of the first Earth-orbiting artificial satellite Sputnik 1 which caught the USA unprepared. The event ignited the Space Race during the Cold War, and led to the USA successfully completing a human landing on the Moon in 1969.

A CAUTIONARY TALE

A Cautionary Tale

- Ted Hoff, Co-Inventor of the Intel i4004 CPU, the World's First commercially available microprocessor:

  "You can be smart and talented, and invent and produce great things, but if you can't demonstrate the Business Value, and Market it and monetize it, you are doomed to fail."

Ted Hoff, Inventor of the Microprocessor

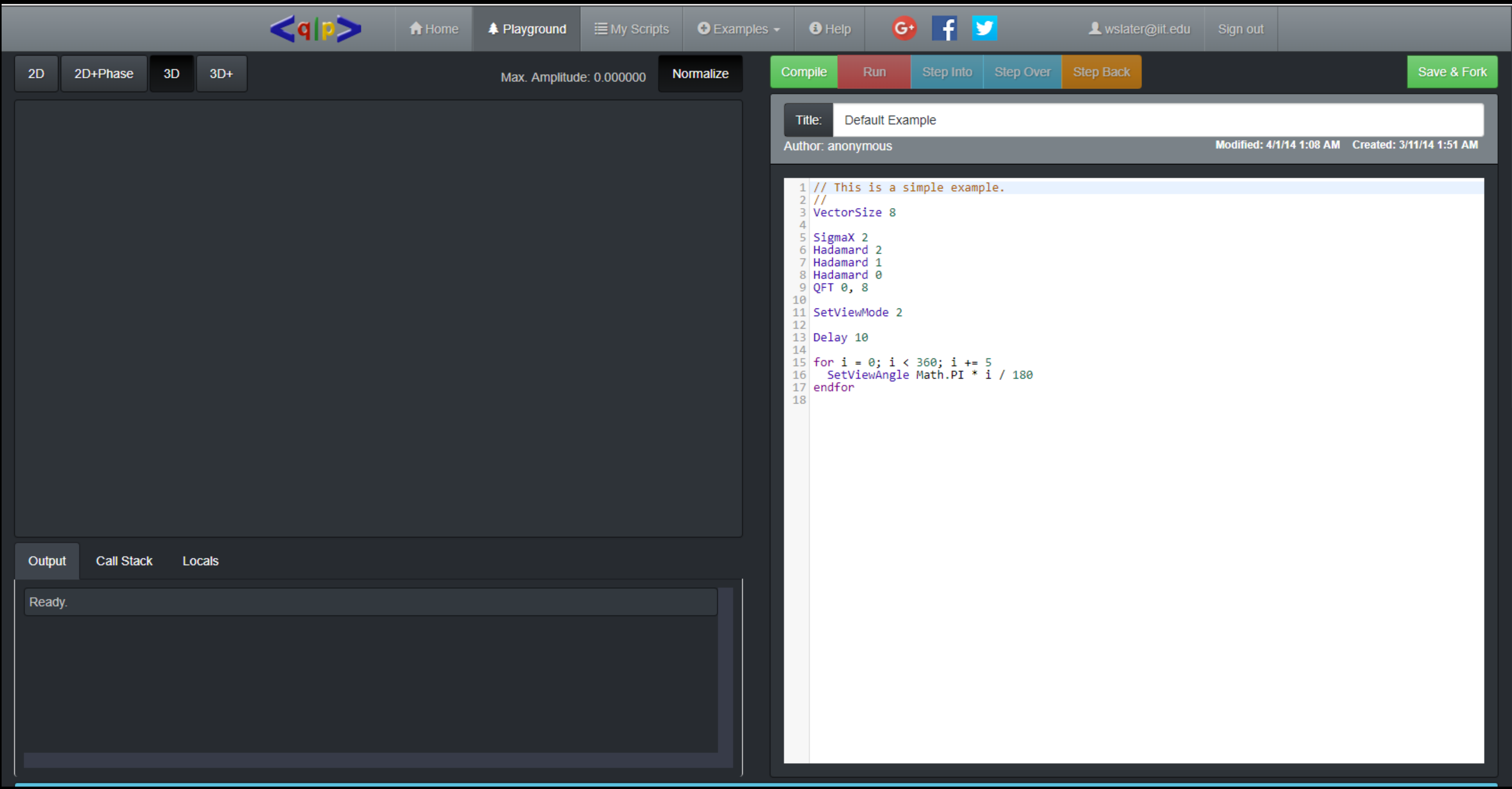
Source: https://www.youtube.com/watch?v=7MgHsgoilQ4&t=80s

A CALL TO ACTION

A Call to Action

- Quantum is the Future of Computing
- Get busy and learn everything you can about Quantum Science and Quantum Technologies
- There are lots of Free Resources
  - Quantum Playground (Free)
  - IBM Q (Free… for now!)
  - Chicago Quantum MeetUp Group (Free)

Quantum Playground



Visit http://quantumplayground.net

IBM Q

Robert Loredo • 2nd
Product Leader, Master Inventor, Blockchain Digital Mentor, Qua...
1d

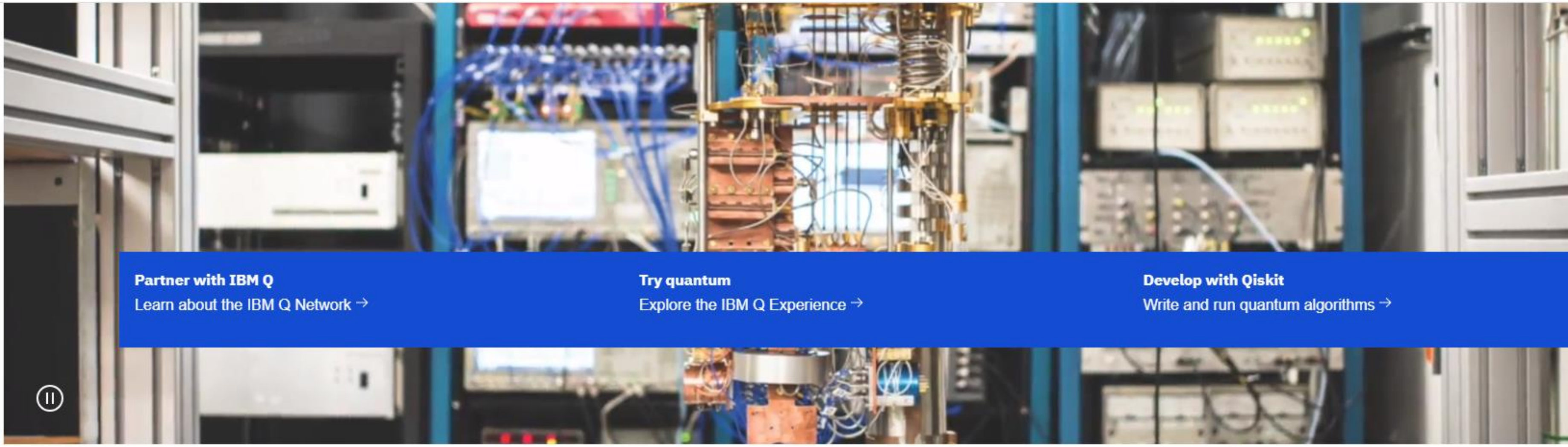
If you haven't tried it out yet, better hurry! So far the #IBMQ Experience has reached 100,000 users, who have run more than 6.5 million experiments. This makes it the most widely used cloud-based quantum system in the world!
https://lnkd.in/ePVExgN
#IBMQ #quantumcomputing #quantum #quantuminformation #engineering #scienceandtechnology #technology #cloud #research #ibm #computing

IBM Research AI
research.ibm.com

IBM Q

IBM

IBM Q | Network | Technology | Learn | Community



IBM Q
The future is quantum

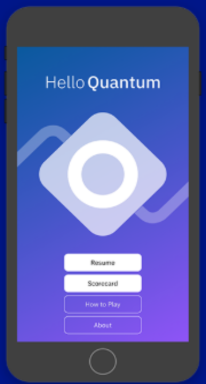
IBM Q is an industry first initiative to build universal quantum computers for business and science. Our cross-disciplinary team is developing scalable quantum systems, and potential applications for the technology we make available today. IBM Q quantum devices are accessed using Qiskit, a modular, open-source programming framework. A worldwide network of Fortune 500 companies, academic institutions, and startups use IBM Q technology and collaborate with IBM Research to advance quantum computing.

Learn more about quantum computing at IBM →

Visit https://www.research.ibm.com/ibm-q/

IBM Q

IBM Q | Network | Technology | Learn | Community



Hello Quantum →

Explore the building blocks of quantum mechanics through puzzles.

Welcome to the IBM Q Experience!

Explore the world of quantum computing! Check out our User Guides and interactive Demos to learn more about quantum principles. Or, dive right in to create and run algorithms on real quantum computing hardware, using the Quantum Composer and QISKit software developer kit.

Start experimenting with a quantum computer

Introducing the IBM Q Experience for Researchers

A community built for individuals who actively contribute to the advancement of the field through peer-reviewed publications. Our goal is to provide quantum researchers with the support, collaboration and tooling they need to do high quality work.

Applications now open!

Visibility for your papers

Priority access to devices

Support letters for research funding

A community built for you!

light

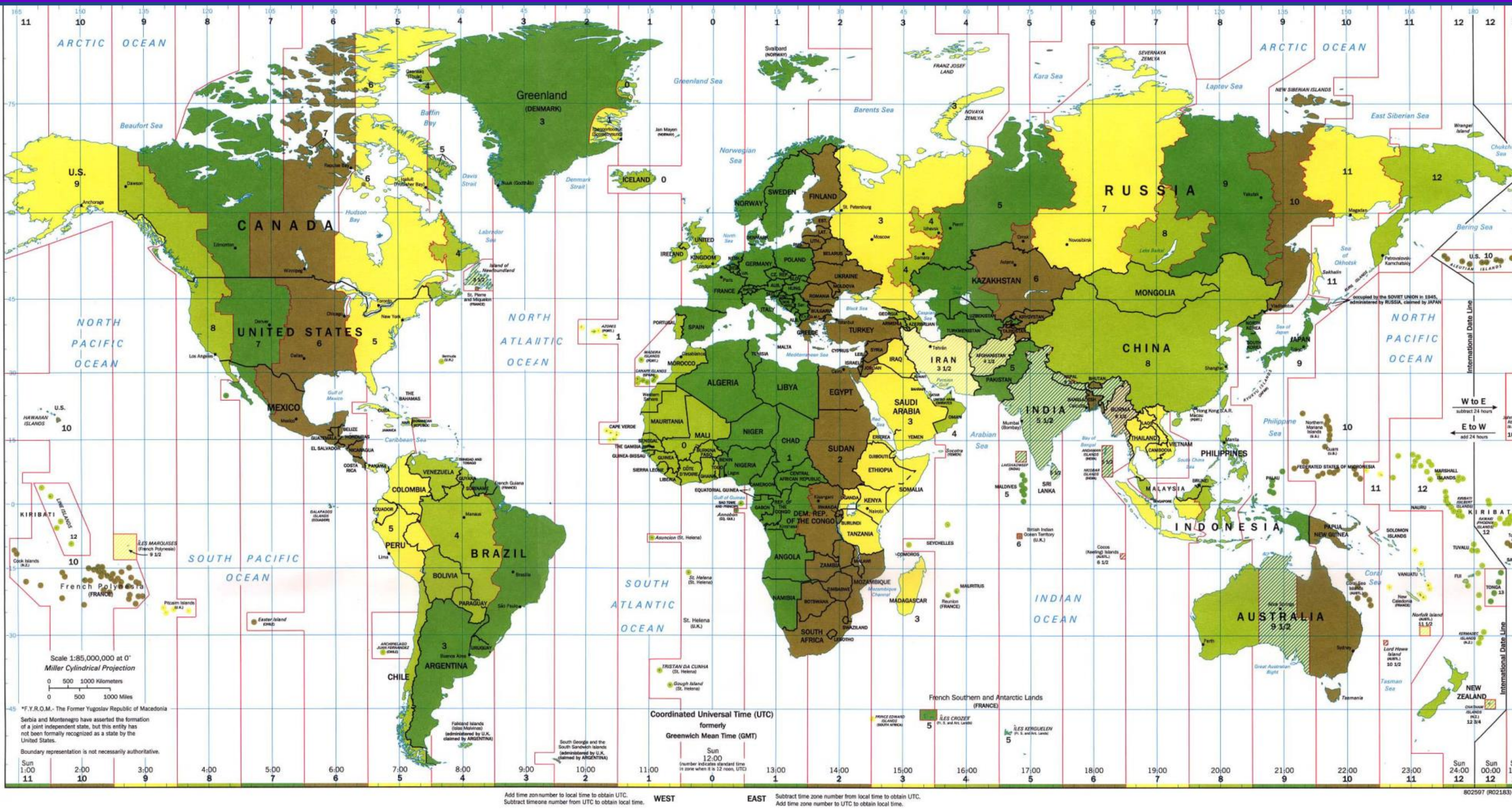
Visit https://www.research.ibm.com/ibm-q/

CONCLUSION

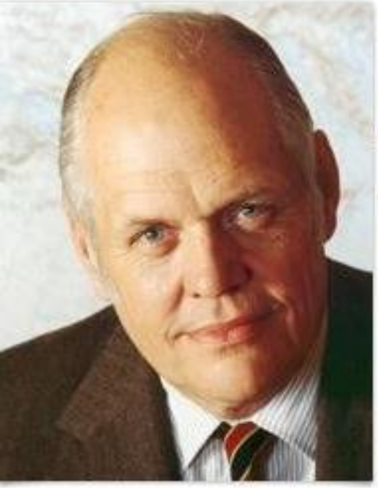
Conclusion

- We covered the following:
  - What is Quantum Computing?
  - Quantum Computing Terminology
  - Some Important Standards Around Computing and the Internet
  - The Formation of Quantum Computing Standards
  - The Potential and Promise of Quantum Computing
  - Quantum Computing – The Downside
  - How and Why Quantum Computing Will Persist, and Rapidly Evolve and Be Adopted
  - A Cautionary Tale
- The Standards being formed by these thought leaders will help to accelerate the maturation, adoption, and widespread use of quantum computing.
- In America, we need a “Sputnik Moment” in Quantum Science and Technology, and we need to get busy and rise.
- Call to Action: Get Busy!

Questions?



ARCTIC OCEAN
Greenland
(DENMARK)
CANADA
UNITED STATES
MEXICO
NORTH PACIFIC OCEAN
NORTH ATLANTIC OCEAN
SOUTH PACIFIC OCEAN
SOUTH ATLANTIC OCEAN
INDIAN OCEAN
BRAZIL
ARGENTINA
CHILE
PERU
COLOMBIA
BOLIVIA
VENEZUELA
RUSSIA
KAZAKHSTAN
MONGOLIA
CHINA
INDIA
IRAN
SAUDI ARABIA
ALGERIA
LIBYA
EGYPT
SUDAN
NIGER
CHAD
MALI
ANGOLA
DEM. REP. OF THE CONGO
SOUTH AFRICA
AUSTRALIA
INDONESIA
PHILIPPINES
JAPAN
NEW ZEALAND
TURKEY
ICELAND
SWEDEN
FINLAND
NORWAY
FRANCE
SPAIN
GERMANY
POLAND
International Date Line
W to E
E to W
Scale 1:85,000,000 at 0°
Miller Cylindrical Projection
Coordinated Universal Time (UTC)
formerly
Greenwich Mean Time (GMT)
WEST
EAST
Add time zone number to local time to obtain UTC.
Subtract time zone number from UTC to obtain local time.
Subtract time zone number from local time to obtain UTC.
Add time zone number to UTC to obtain local time.
802597 (R02183) 6-98



"Software comes from heaven when you have good hardware."

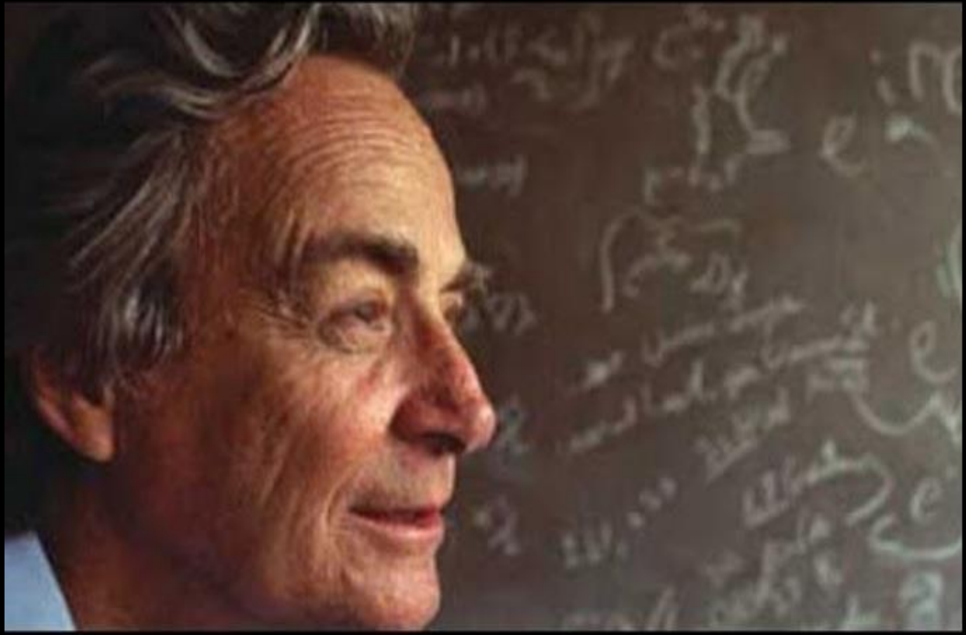
Ken Olsen

"One of life's most painful moments comes when we must admit that we didn't do our homework, that we are not prepared."

Merlin Olsen

If you think you understand quantum mechanics, you don't understand quantum mechanics.

— *Richard P. Feynman* —



William Favre Slater, III

- 312-758-0307
- slater@billslater.com
- williamslater@gmail.com
- http://billslater.com/interview
- 1515 W. Haddon Ave., Unit 309
  Chicago, IL 60642
  United States of America

William Favre Slater, III

REFERENCES

References

- Ahsan, M., Meter, R V., and Kim, J. (2015). Designiing a Million-Qubit Quantum Computer Using a Resource Performance Simulator. A scholarly article published at the ACM in December 2015. Retrieved from: https://tinyurl.com/ya2q92xa.
- Da Silva, W. (2015). Quantum computer coding in silicon now possible. Published at the University of New South Wales Newsroom on November 17, 2015. Retrieved from: https://newsroom.unsw.edu.au/news/science-tech/quantum-computer-coding-silicon-now-possible .
- DeAngelis, S. (2014). A Glossary of Quantum Computing Terms. Retrieved from https://www.enterrasolutions.com/blog/glossary-quantum-computing-terms/ .
- Fedorov, A. K. , Kiktenko, E. O., and Lvovsky, A. I. (2018). Quantum computers put blockchain security at risk. Published November 19, 2018 in Nature. Retreived from: https://www.nature.com/articles/d41586-018-07449-z .
- Gerschenfeld, N. and Chuang, I. L. (1998). Quantum Computing with Molecules. Published in the June 1998 edition of Scientific American magazine. Retrieved from: http://cba.mit.edu/docs/papers/98.06.sciqc.pdf .
- Gomes, L. (2018). Quantum Computers Strive to Break Out of the Lab. Published at IEEE Spectrum on March 22, 2018 Retrieved from https://spectrum.ieee.org/computing/hardware/quantum-computers-strive-to-break-out-of-the-lab.
- Herman, A. (2018). Winning the Race in Quantum Computing. Published in American Affairs Journal. Retrieved from: https://americanaffairsjournal.org/2018/05/winning-the-race-in-quantum-computing/ .
- Hoff, T. (2009). Lecture by Ted Hoff at U.C. Berkley. Located at: https://www.youtube.com/watch?v=7MgHsgoilQ4&t=80s .
- Hurley, W. (2018). Quantum Computing Standards. A webinar presented on April 24, 2018 and located at https://www.youtube.com/watch?v=qKt7dOf4pXY&t=7s .
- IBM. (2018). IBM Q. Located at https://www.research.ibm.com/ibm-q/.

References

- IEEE. (2018). IEEE P7130 - IEEE Nomenclature Standard. Quantum Computing Working Group. Located at: https://standards.ieee.org/develop/project/7130.html .
- IEEE. (2018). IEEE P7131 - IEEE Benchmarking Standard. Quantum Computing Working Group. Located at: https://standards.ieee.org/develop/project/7131.html .
- Kholodov, I. (2009). The von Neumann Computer Model. From the CIS-77 course at Bristol Community College. Retrieved from: http://www.c-jump.com/CIS77/CPU/VonNeumann/lecture.html .
- Klarreich, E. (2018). Graduate Student Solves Quantum Verification Problem. Published in Quanta Magazine, October 8, 2018. Retrieved from https://www.quantamagazine.org/graduate-student-solves-quantum-verification-problem-20181008/ .
- Miller, S. (2018). DARPA digs into the details of practical quantum computing. Retrieved from: https://gcn.com/articles/2018/07/12/darpa-quantum-architecture.aspx .
- New York Times. (2018). The next tech talent shortage: Quantum computing researchers. Retrieved from https://indianexpress.com/article/technology/science/the-next-tech-talent-shortage-quantum-computing-researchers-5412552/ .
- Panetta, K. (2017). The CIO's Guide to Quantum Computing. Published November 29, 2017. Retrieved from https://www.gartner.com/smarterwithgartner/the-cios-guide-to-quantum-computing/ .
- Quantum Computing Playground. (2014). Located at http://www.quantumplayground.net/#/home .
- Sattel, S. (2016). The Future of Computing - Quantum & Qubits. Retrieved from: https://www.autodesk.com/products/eagle/blog/future-computing-quantum-qubits/ .
- Wikipedia. (2011). Quantum Machine. Retrieved from: https://en.wikipedia.org/wiki/Quantum_machine .
- Wikipedia. (2018). Article on Quantum Superposition. Retrieved from https://en.wikipedia.org/wiki/Quantum_superposition.
- Wilson, L. (2015). The Rise of Quantum Computers - The Current State of Cryptographic Affairs. http://www.activecyber.net/rise-quantum-computers-current-state-cryptographic-affairs/ .