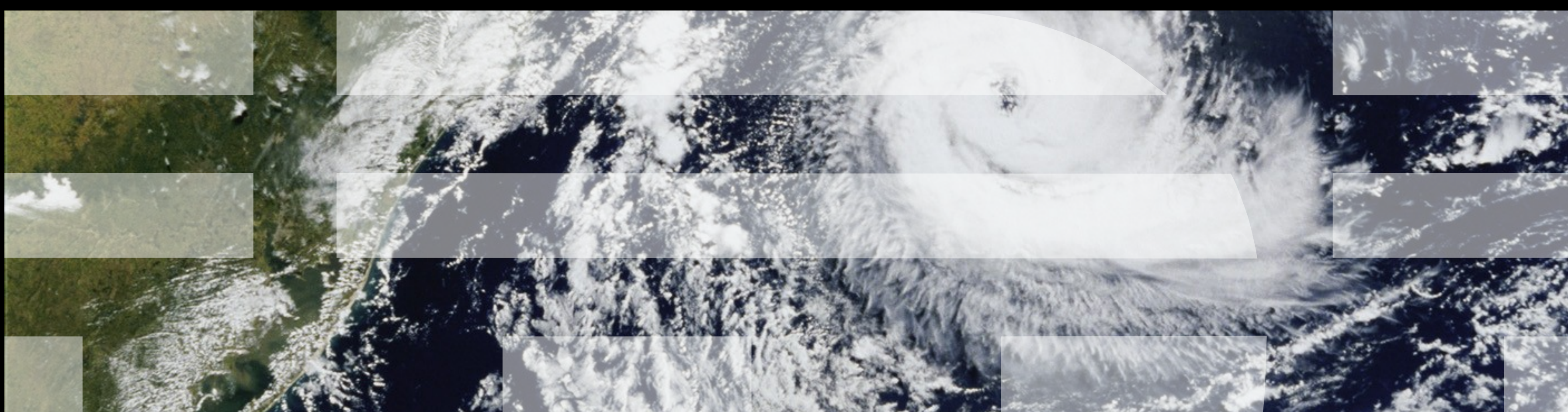
Paul E. McKenney, IBM Distinguished Engineer, Linux Technology Center
Member, IBM Academy of Technology
Beaver BarCamp 18, April 7, 2018

How Will Linux Handle Quantum Computing?

An entangled superposition of views



Overview

- Who cares about quantum computing?
- What is so great about quantum computing?
- Quantum computing technical trends
- Trouble with thermodynamics
- What is quantum computing's killer app?
- Quantum computing and Linux?
- Summary

- Notes:
  - Quantum communication/encryption already relatively advanced
  - For programming quantum computers, see IBM-Q or get a D-Wave

Who Cares About Quantum Computing?

Who Cares About Quantum Computing?

- D-Wave Systems: Champion in qubit count
- Google: Champion in QC memory, 72-qubit prototype
- Intel: Investing $50M in partnership w/Google, NASA, USRA
  - Silicon-based spin-qubit hardware prototyped in early 2018
    - High temperature (1K) but also higher error rates, 49 qubits
- Microsoft: Champion in QC languages
  - Has proposed a new topological qubit
- IBM: Champion in QC to the masses
  - And **real** qubits, not the cheap imitations that you might find elsewhere
  - http://research.ibm.com/ibm-q/
  - https://github.com/qiskit
- However, current QC offerings are a bit primitive
  - Think 1940s computers...

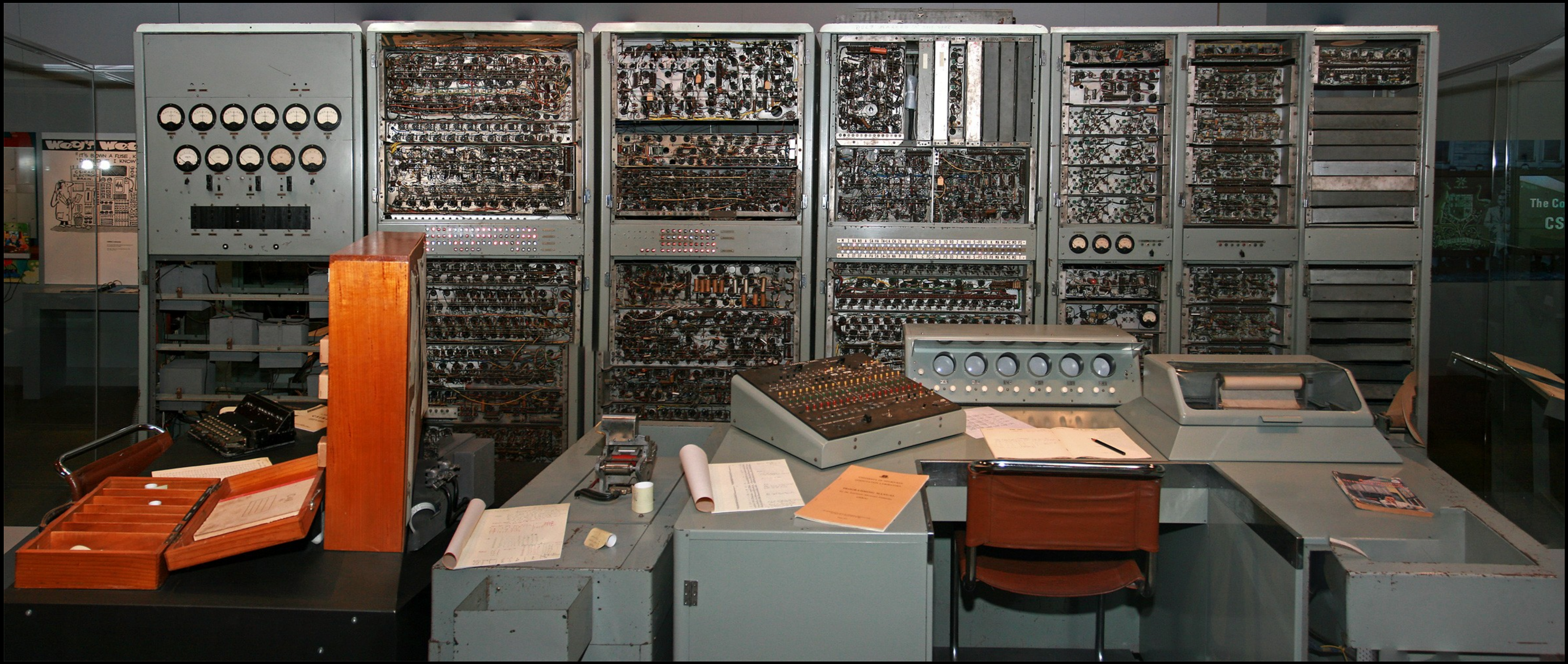
What Did mid-1940s Computers Look Like?

https://en.wikipedia.org/wiki/Z4_(computer)
Photo by Clemens Pfeiffer under CC by 2.5

What Did mid-1940s Computers Look Like?

- 32-bit floating-point arithmetic (decimal input and output)
- Punched film input (and 35mm film at that)
- 2,500 relays (not transistors, or even tubes)
- 64 words of 32-bit mechanical memory
- CPU core clock frequency of... 40Hz
  - About 2.5 octaves below middle C
- Energy-efficient design sips only 4kW
- 400 milliseconds addition, 3 seconds multiplication
- First computer to be sold and delivered in working condition

What Did late-1940s Computers Look Like?



https://en.wikipedia.org/wiki/CSIRAC
Photo by John O'Neill under GNU FDL v1.2

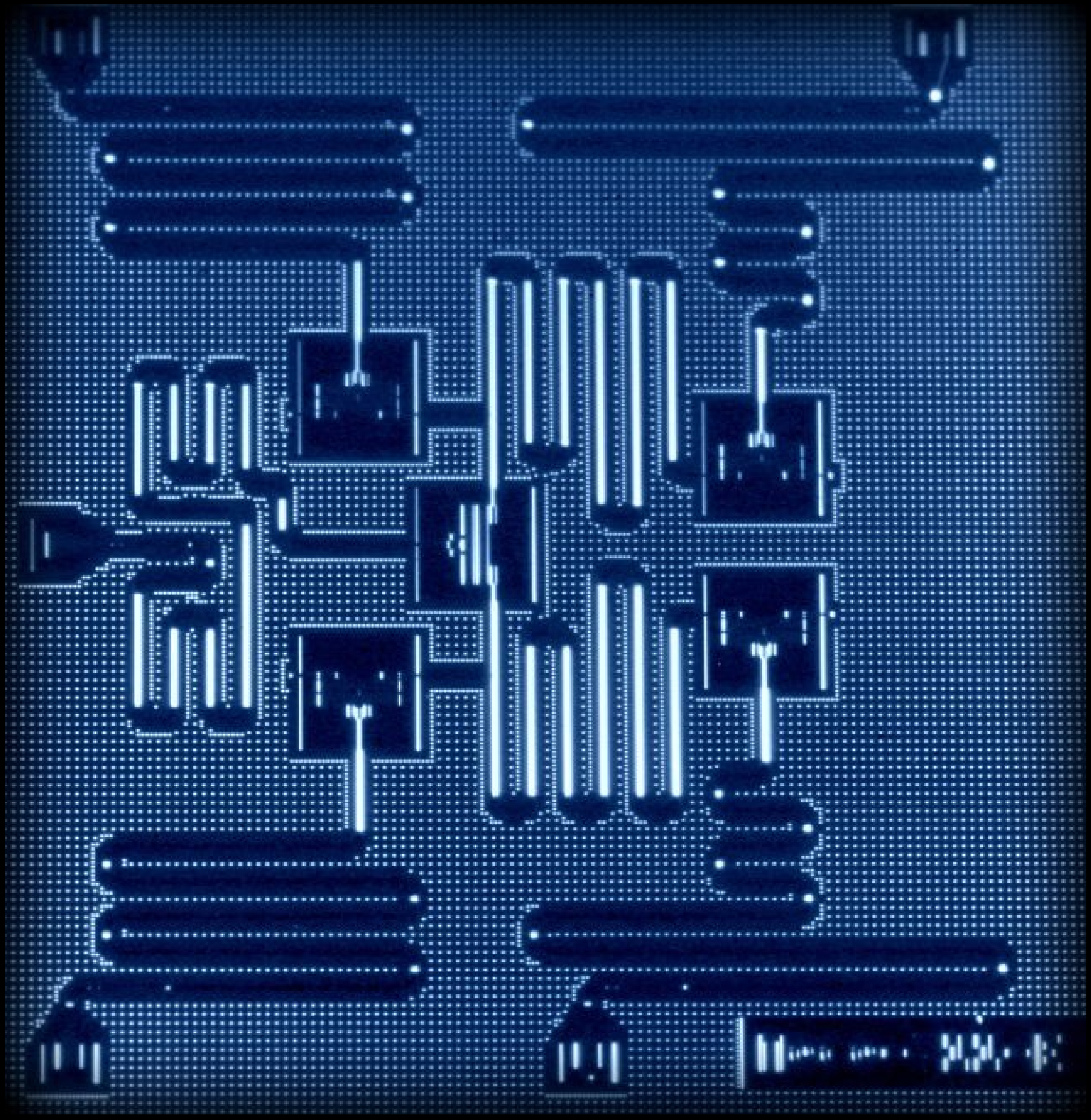
What Did late-1940s Computers Look Like?

- CSIRAC: Oldest intact electronic stored-program computer
  - Operational in November 1949 at University of Melbourne
- 2,000 Vacuum tubes: Each an incandescent lightbulb in size
  - And less capable than a transistor: Need more tubes than transistors
- 768 words of memory, 20 bits each, in mercury delay lines
  - Hence “surviving” rather than operational
    - Modern safety regs unforgiving of metallic mercury & exposed 600V wiring
- CPU core clock frequency of... 1KHz
  - Almost two octaves above middle C
- Energy-efficient design sips only 30kW

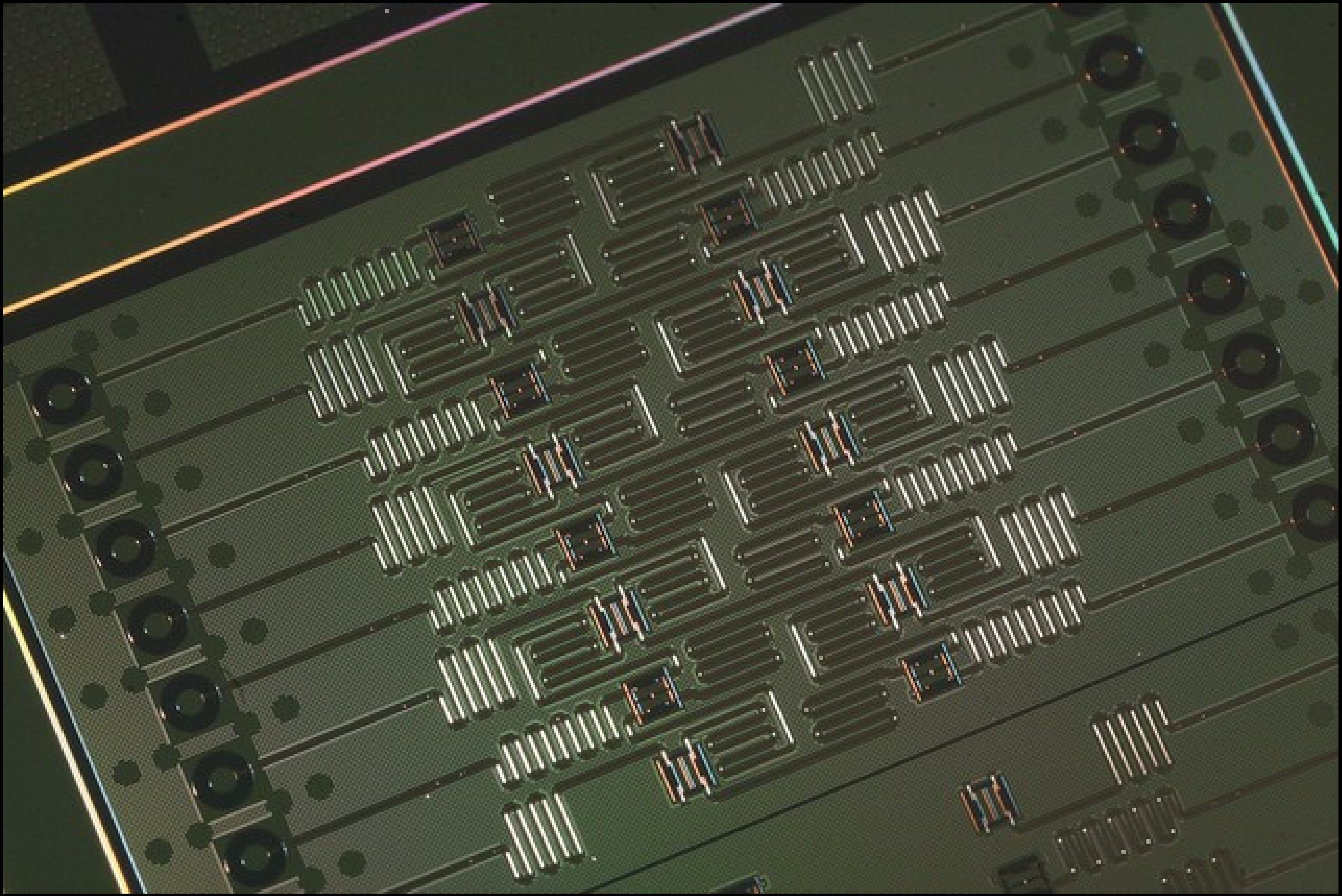
What Did late-1940s Computers Look Like?

- CSIRAC: Oldest intact electronic stored-program computer
  - Operational in November 1949 at University of Melbourne
- 2,000 Vacuum tubes: Each an incandescent lightbulb in size
  - And less capable than a transistor: Need more tubes than transistors
- 768 words of memory, 20 bits each, in mercury delay lines
  - Hence “surviving” rather than operational
    - Modern safety regs unforgiving of metallic mercury & exposed 600V wiring
- CPU core clock frequency of... 1KHz
  - Almost two octaves above middle C
- Energy-efficient design sips only 30kW (about 300 people)
- Present-day QC systems are similarly crude

IBM's Five-Qubit Quantum Computer

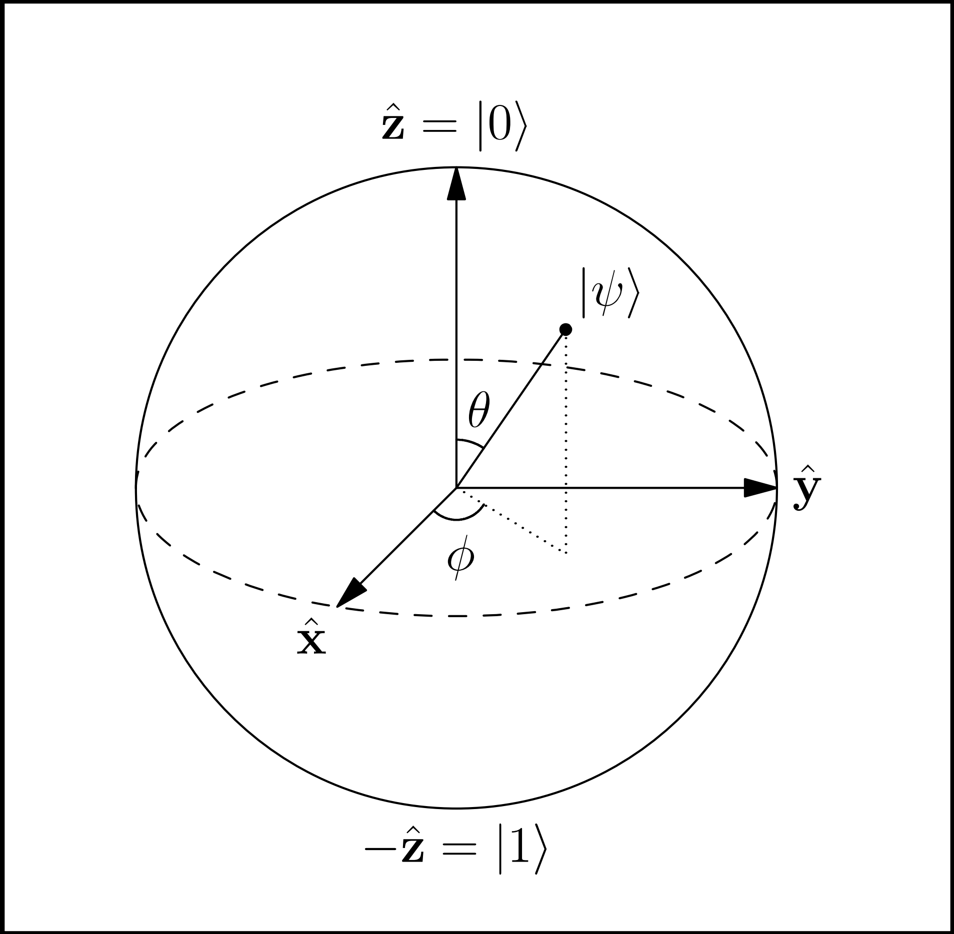


IBM's Five-Qubit Quantum Computer (And Now 16!!!)



What is so Great About Quantum Computing???

Superposition in Qubit as Bloch Sphere



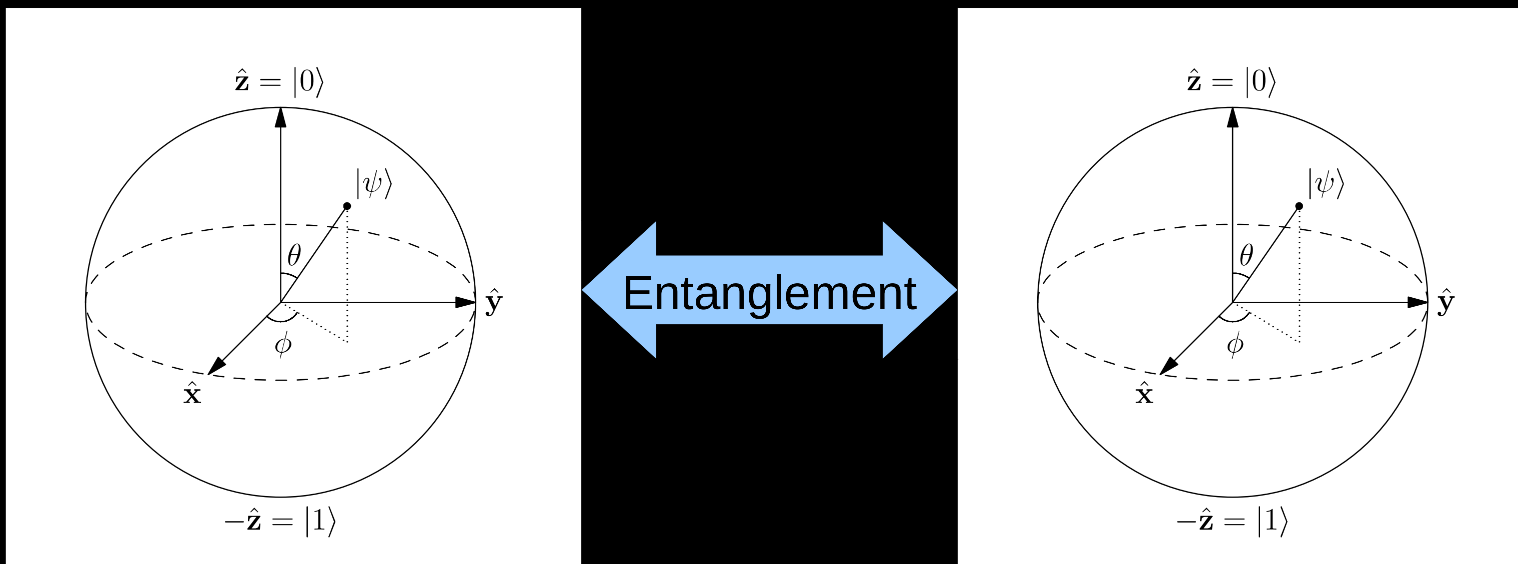
Qubit is a pair of FP #s, but measurement projects onto z axis
http://research.ibm.com/ibm-q/

Superposition by Itself is Unexciting

- All it gets you is an extremely inaccurate, slow, and error-prone reinvention of a small subset of the capabilities of this 1960s analog computer
- Which was emphatically obsoleted by classic computing

Kierano, public domain

Entanglement!!! Entangled Qubits as Bloch Spheres



Entanglement can act sort of like constraints between groups of qubits
https://www.smbc-comics.com/comic/the-talk-3
https://xkcd.com/1240/
No one really knows how this works: https://www.scottaaronson.com/blog/?p=3628

Quantum Computing Technical Trends

QC Trends: D-Wave Number of “Qubits”

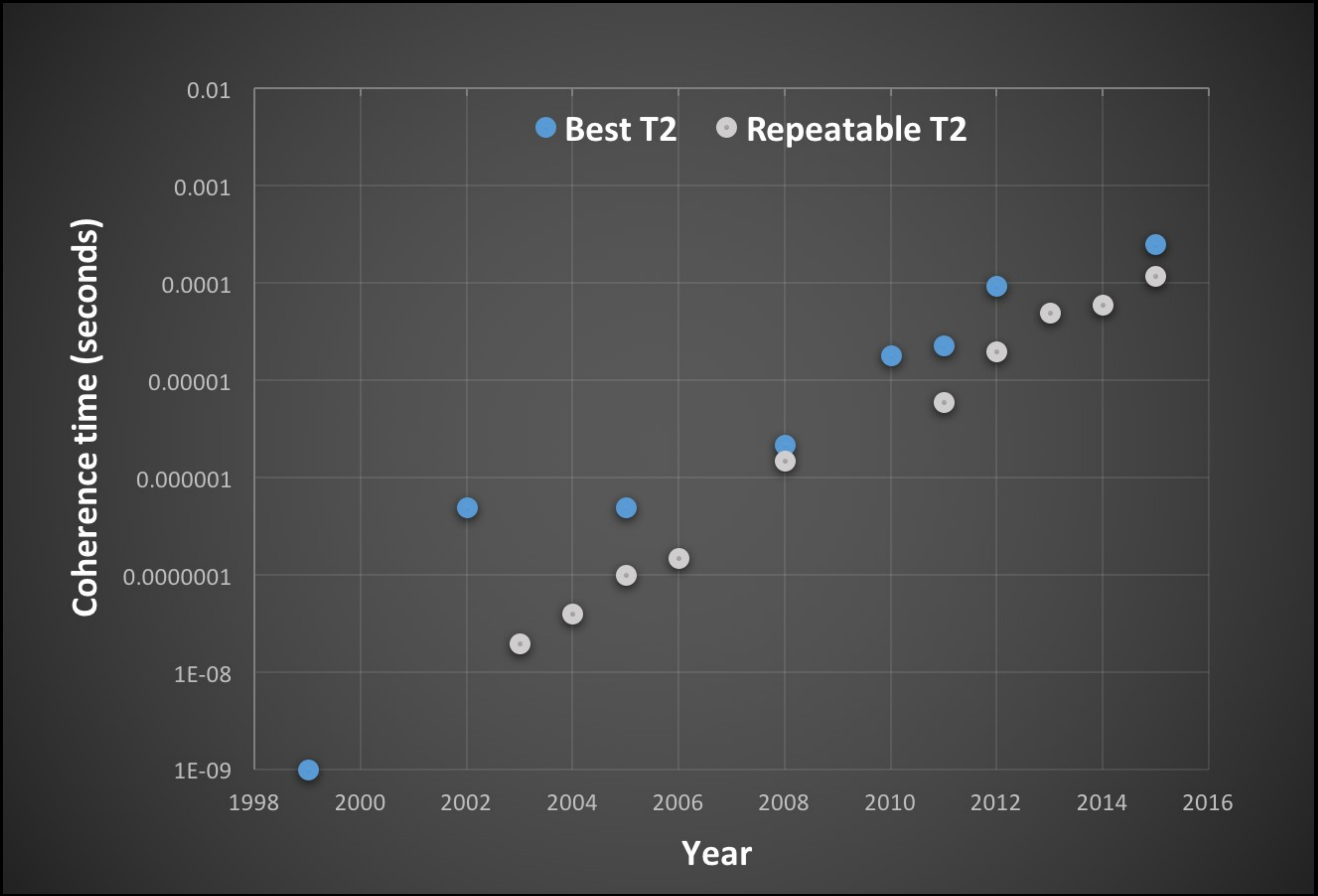
System	Availability	# Qubits	Years per Doubling
D-Wave One	May 2011	128	1.4
D-Wave Two	May 2013	512	1.9
D-Wave 2X	August 2015	1152	1.7
D-Wave 2000Q	January 2017	2048	–

Moore's-Law-style exponential growth
IBM-Q supports 5 X 20 50 full-function qubits, Google prototyped 72
IBM-Q doubling every 8 *months*, sustainable?

QC Trends: Limits on Number of Qubits

- Qubits are more like CPU than like memory
  - Each qubit must be connected to its own signal generator
- One million qubits means 1M wires to 1M signal generators
  - Tens of thousands of $US per signal generator
    - But it should be possible to create cheaper signal-generator ASICs
  - 1M wires each conduct heat down to the quantum computer
    - Currently from room temperature but perhaps from 4K in the future
  - Need cheap small low-temperature energy-efficient signal generators!
    - **Lots** of them!!!
- Per-qubit error rates range from 90% to 99%
  - Need something more like 99.99%
  - Otherwise almost all qubits are devoted to quantum error correction
  - Which means additional qubits provide almost no benefit

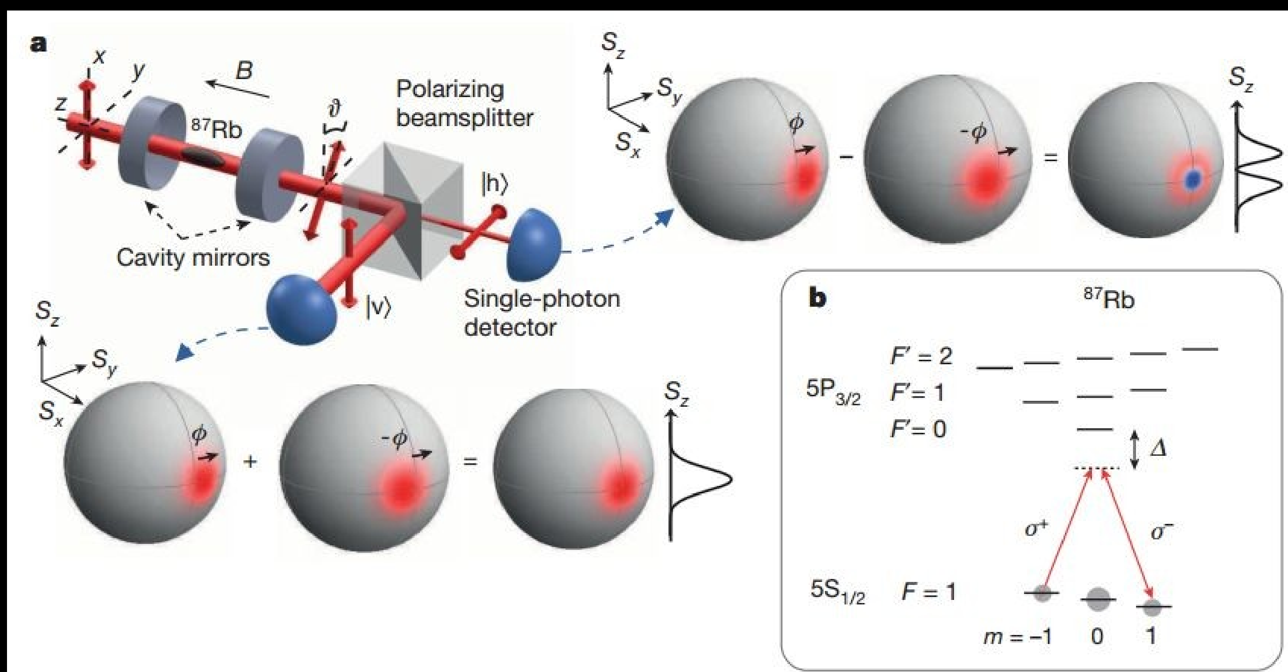
QC Trends: Coherence Time (DRAM, But No Refresh)



Ten seconds in 2027? 39 *minutes* but...

QC Trends: Number of Entangled Qubits

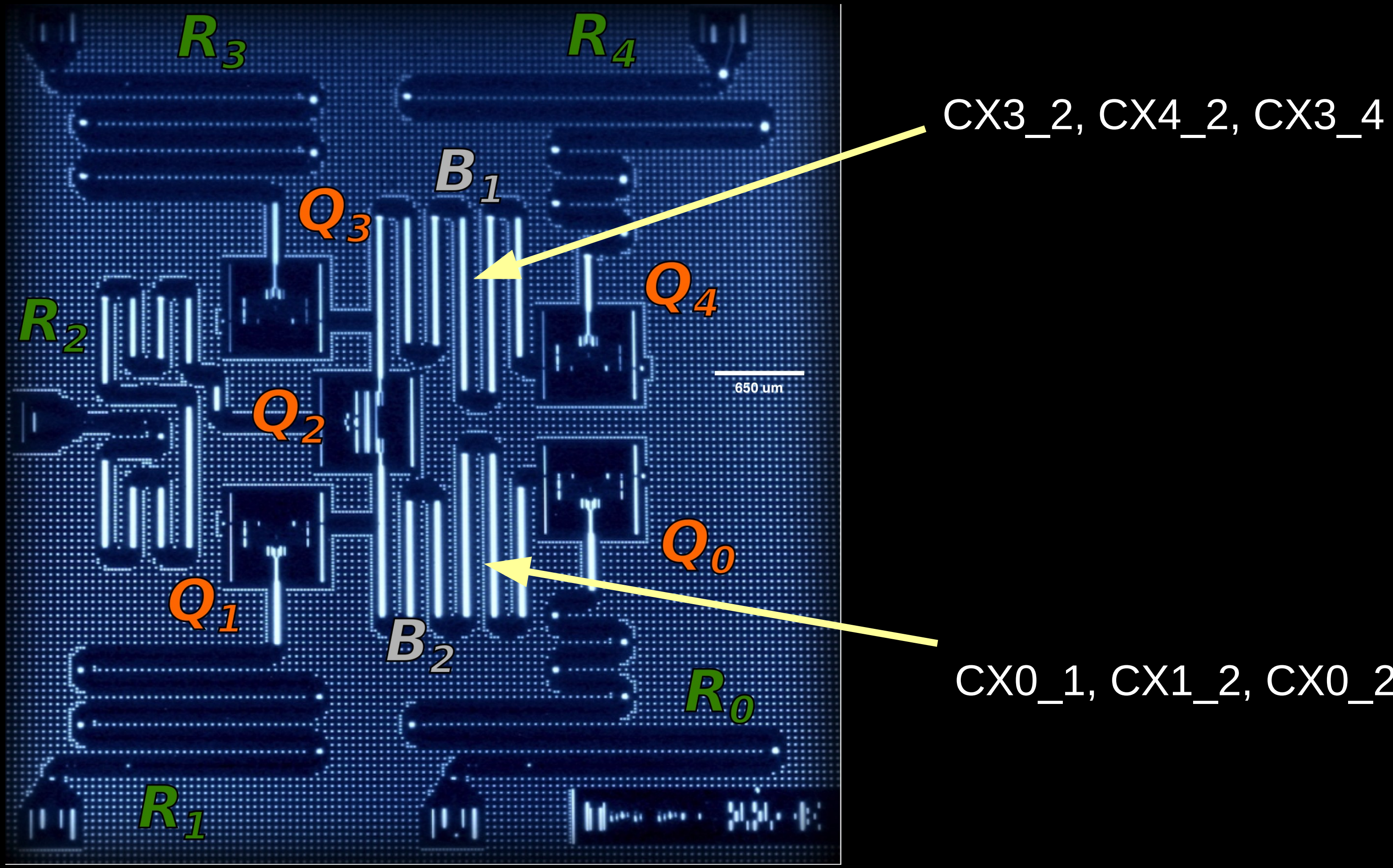
- IBM-Q: restricted entanglement among 5X 16 qubits
- Claims of up to 8-qubit D-Wave entanglement
- Up to 3,000 rubidium atoms entangled in lab experiment
  - But not clear how to make useful computer of low-temperature gas
  - Reproducing this in QC would greatly build confidence!



Quantum Computing Technical Trends: Volume

- Exponential Moore's-Law-like progress:
  - Number of qubits
  - Coherence times
- Jury still out on entanglement
- But connectivity is also important: “quantum volume”
  - Number of qubits
  - Number of operations until decoherence
  - Connectivity
  - Parallelism
  - ***Error rate!!!***
    - https://www.ibm.com/blogs/research/2017/07/increase-quantum-iq/
    - https://dal.objectstorage.open.softlayer.com/v1/AUTH_039c3bf6e6e54d76b8e66152e2f87877/community-documents/quatnum-volumehp08co1vbo0cc8fr.pdf

Error Rate Example: ibmqx2 Connectivity



Quantum Volume: Error Rates for ibmqx2, Percent

	Q0	Q1	Q2	Q3	Q4	
Gate Error	0.2	0.1	0.2	0.2	0.1	
Gate Fidelity	99.8	99.9	99.8	99.8	99.9	
Readout Error	4.5	3.6	2.0	1.6	2.5	
Readout Fidelity	95.5	96.4	98.0	98.4	97.5	
Multi-Qubit Gate Error (Entanglement)						
	CX0_1	CX0_2	CX1_2	CX3_2	CX3_4	CX4_2
Error	3.5	4.1	3.3	2.8	2.2	2.7
Fidelity	96.5	95.9	97.3	97.2	97.8	97.3

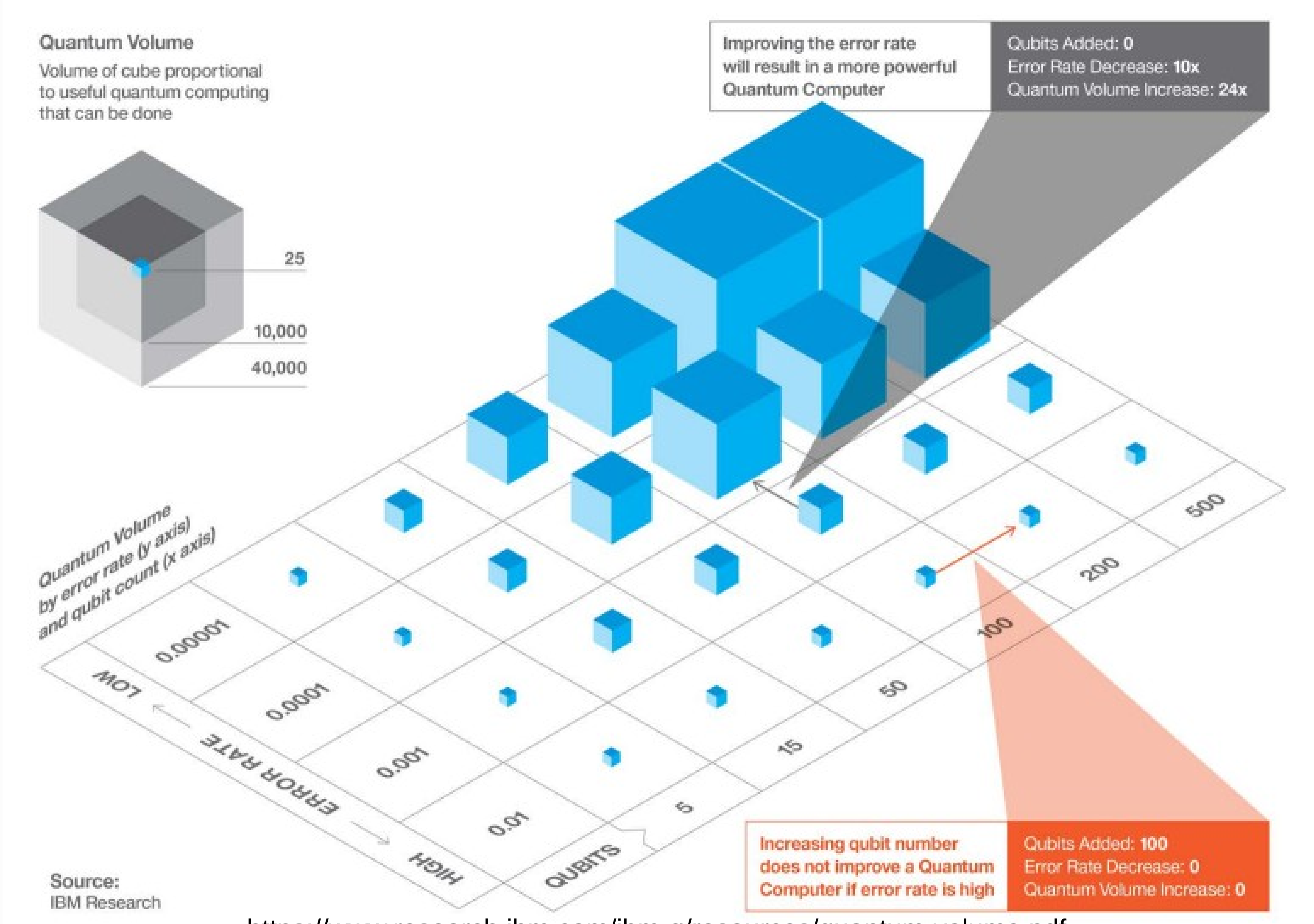
From data calibration on February 13, 2018

Quantum Volume: Error Rates for ibmqx2, Percent Unfortunately, We Need More Like 99.99%!!!

	Q0	Q1	Q2	Q3	Q4	
Gate Error	0.2	0.1	0.2	0.2	0.1	
Gate Fidelity	99.8	99.9	99.8	99.8	99.9	
Readout Error	4.5	3.6	2.0	1.6	2.5	
Readout Fidelity	95.5	96.4	98.0	98.4	97.5	
Multi-Qubit Gate Error (Entanglement)						
	CX0_1	CX0_2	CX1_2	CX3_2	CX3_4	CX4_2
Error	3.5	4.1	3.3	2.8	2.2	2.7
Fidelity	96.5	95.9	97.3	97.2	97.8	97.3

From data calibration on February 13, 2018

Error Rate Is Most Serious Obstacles to Moore's-Law-Style Improvements to Quantum Computers!!!



https://www.research.ibm.com/ibm-q/resources/quantum-volume.pdf

Error Rate Is Most Serious Obstacles to Moore's-Law-Style Improvements to Quantum Computers!!!

- Also, ***never*** forget the three laws of thermodynamics!
  - Because they sure won't forget ***you!!!***

Trouble With Thermodynamics

Trouble With Thermodynamics: The Three Laws

1) Energy is conserved
   - In English: ***You cannot win***

Trouble With Thermodynamics: The Three Laws

1) Energy is conserved
   – In English: ***You cannot win***

2) Entropy increases in closed systems
   – In English: ***You cannot break even***

Trouble With Thermodynamics: The Three Laws

1) Energy is conserved
   - In English: ***You cannot win***

2) Entropy increases in closed systems
   - In English: ***You cannot break even***

3) Entropy approaches a constant value as temperature approaches absolute zero
   - In English: ***You cannot get out of the game***

Trouble With Thermodynamics: The Three Laws

1) Energy is conserved
   - In English: ***You cannot win***

2) Entropy increases in closed systems
   - In English: ***You cannot break even***

3) Entropy approaches a constant value as temperature approaches absolute zero
   - In English: ***You cannot get out of the game***

- Thermodynamics is to physical-world engineering as the halting problem is to computer science:
  - “The answer is **NO**!!! What was the question?”

Trouble With Thermodynamics: The Three Laws

1) Energy is conserved
   - In English: ***You cannot win***

2) Entropy increases in closed systems
   - In English: ***You cannot break even***

3) Entropy approaches a constant value as temperature approaches absolute zero
   - In English: ***You cannot get out of the game***

- Thermodynamics is to physical-world engineering as the halting problem is to computer science:
  - "The answer is **NO**!!! What was the question?"
- Key point: IBM-Q operates at a temperature of 0.015K
  - In contrast, helium boils at the tropical temperature of 4.2K
  - ***Significant energy is therefore required for refrigeration***

Trouble With Thermodynamics: Keeping it Cool

	T (K)	C_p	Theoretical Minimum Power per Watt Waste Heat (W)
Dry Ice	195	1.990	0.5
Liquid Nitrogen	77	0.356	2.8
Liquid Hydrogen	20	0.073	23.7
Liquid Helium	4	0.0138	72.3
IBM Q	0.015	0.000051	19,500.0

19.5kW is admittedly less than two-thirds of CSIRAC's consumption!

Trouble With Thermodynamics: Keeping it Cool

	T (K)	C_p	Theoretical Minimum Power per Watt Waste Heat (W)
Dry Ice	195	1.990	0.5
Liquid Nitrogen	77	0.356	2.8
Liquid Hydrogen	20	0.073	23.7
Liquid Helium	4	0.0138	72.3
IBM Q	0.015	0.000051	19,500.0

19.5kW is admittedly less than two-thirds of CSIRAC's consumption!
But there are limits to Helium-3 availability

Trouble With Thermodynamics: Keeping it Cool

	T (K)	C_p	Theoretical Minimum Power per Watt Waste Heat (W)
Dry Ice	195	1.990	0.5
Liquid Nitrogen	77	0.356	2.8
Liquid Hydrogen	20	0.073	23.7
Liquid Helium	4	0.0138	72.3
IBM Q	0.015	0.000051	19,500.0

19.5kW is admittedly less than two-thirds of CSIRAC's consumption!
But there are limits to Helium-3 availability
Which is manufactured in nuclear reactors...

IBM

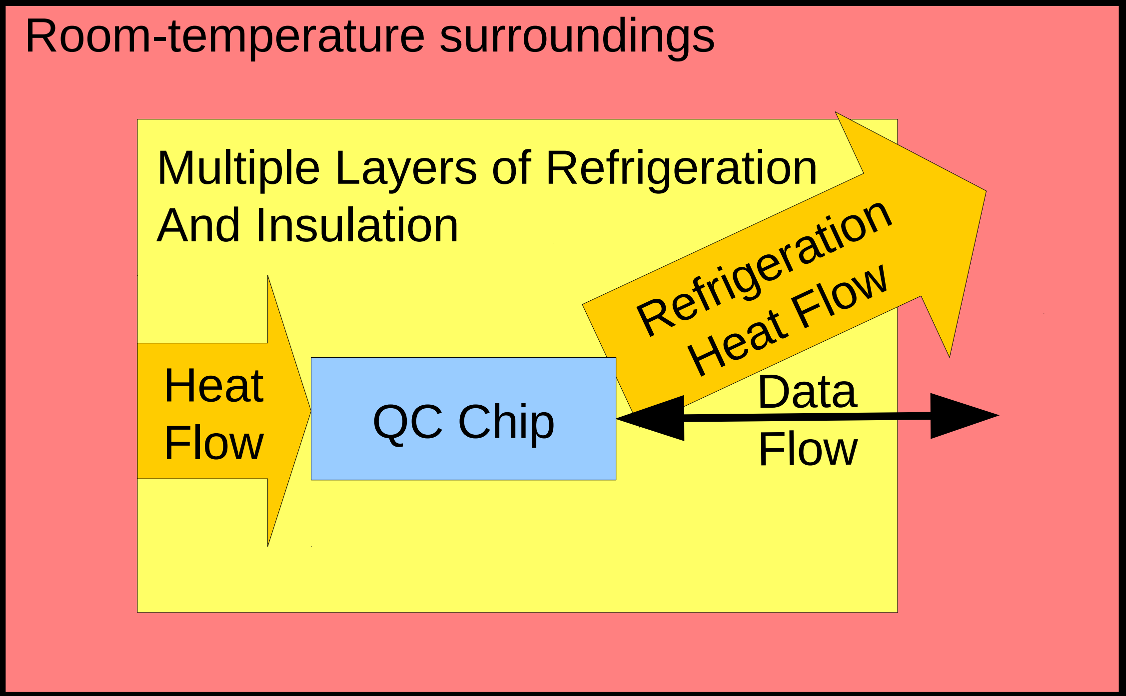
Trouble With Thermodynamics: Keeping it Cool

	T (K)	C_p	Theoretical Minimum Power per Watt Waste Heat (W)
Dry Ice	195	1.990	0.5
Liquid Nitrogen	77	0.356	2.8
Liquid Hydrogen	20	0.073	23.7
Liquid Helium	4	0.0138	72.3
IBM Q	0.015	0.000051	19,500.0

19.5kW is admittedly less than two-thirds of CSIRAC's consumption!
But there are limits to Helium-3 availability
Which is manufactured in nuclear reactors...
And 1 milliwatt per 100 qubits is 19.5MW per 100M qubits...

But Aren't QC Operations Zero Energy Cost???

But Aren't QC Operations Zero Energy Cost??? Yes, In Theory, But...



Heat is conducted along wires, and use of light for data delivers energy
Liquid surroundings transport heat via convection
Vacuum chambers transport heat via radiation
Initialization and readout of quantum state generates waste heat

IBM

Trouble With Thermodynamics: Keeping it Cool

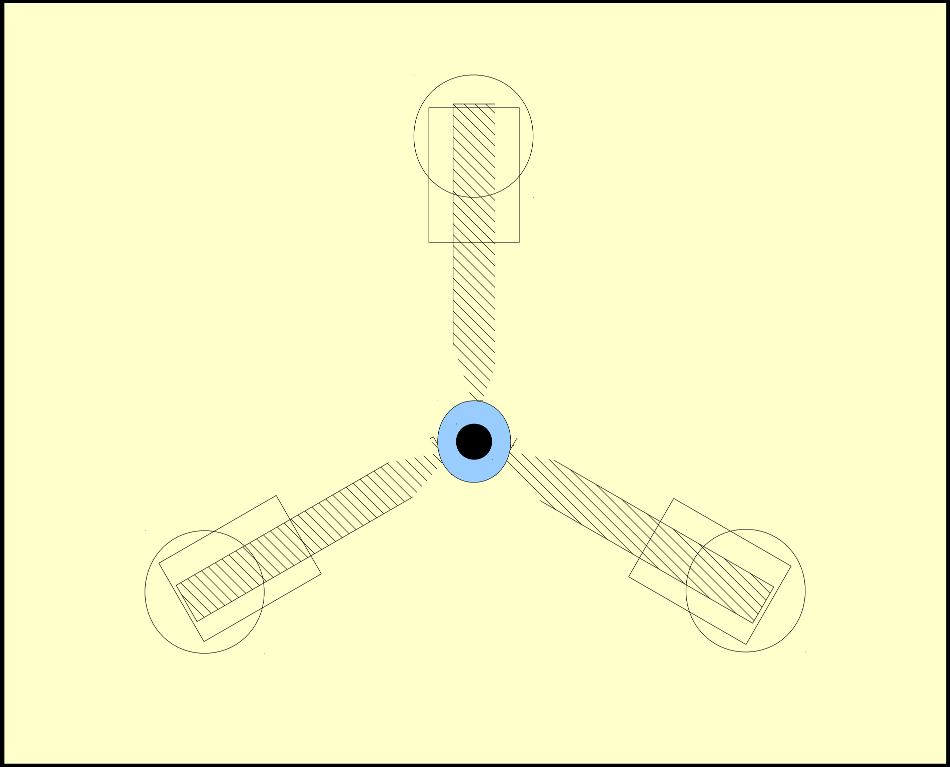
	T (K)	C_p	Theoretical Minimum Power per Watt Waste Heat (W)
Dry Ice	195	1.990	0.5
Liquid Nitrogen	77	0.356	2.8
Liquid Hydrogen	20	0.073	23.7
Liquid Helium	4	0.0138	72.3
IBM Q	0.015	0.000051	19,500.0

And suppose further progress requires even lower temperatures?

Trouble With Thermodynamics: Keeping it Cool

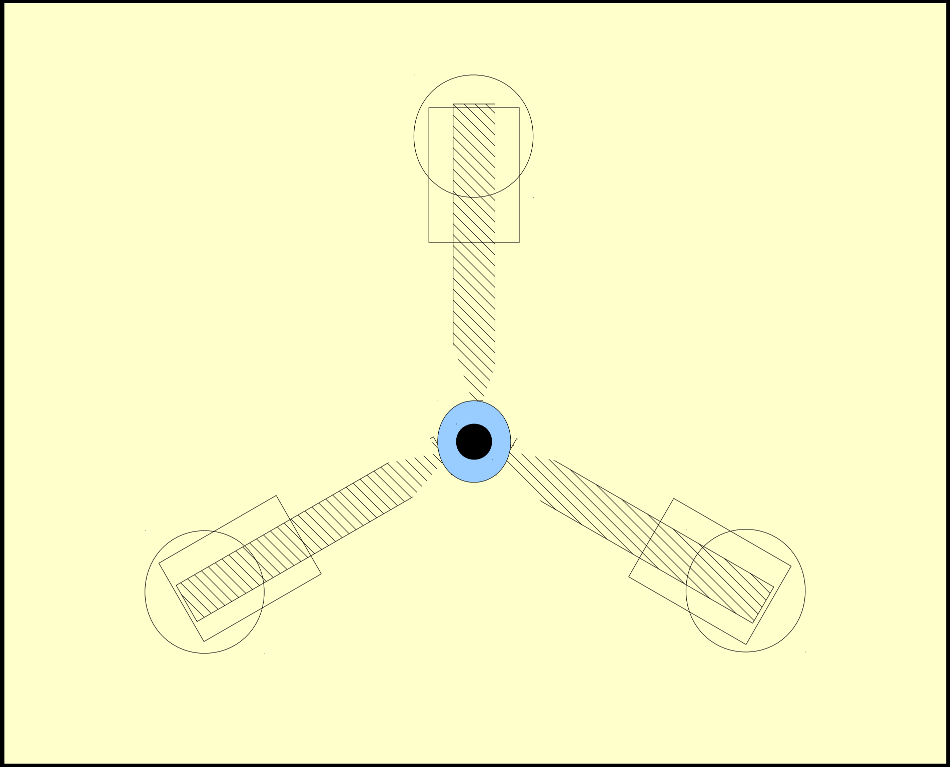
	T (K)	C_p	Theoretical Minimum Power per Watt Waste Heat (W)
Dry Ice	195	1.990	0.5
Liquid Nitrogen	77	0.356	2.8
Liquid Hydrogen	20	0.073	23.7
Liquid Helium	4	0.0138	72.3
IBM Q	0.015	0.000051	19,500.0
Bose-Einstein Condensate (BEC)	0.00000017	0.00000000062	1,605,882,351.9

Trouble With Thermodynamics: Keeping it Cool



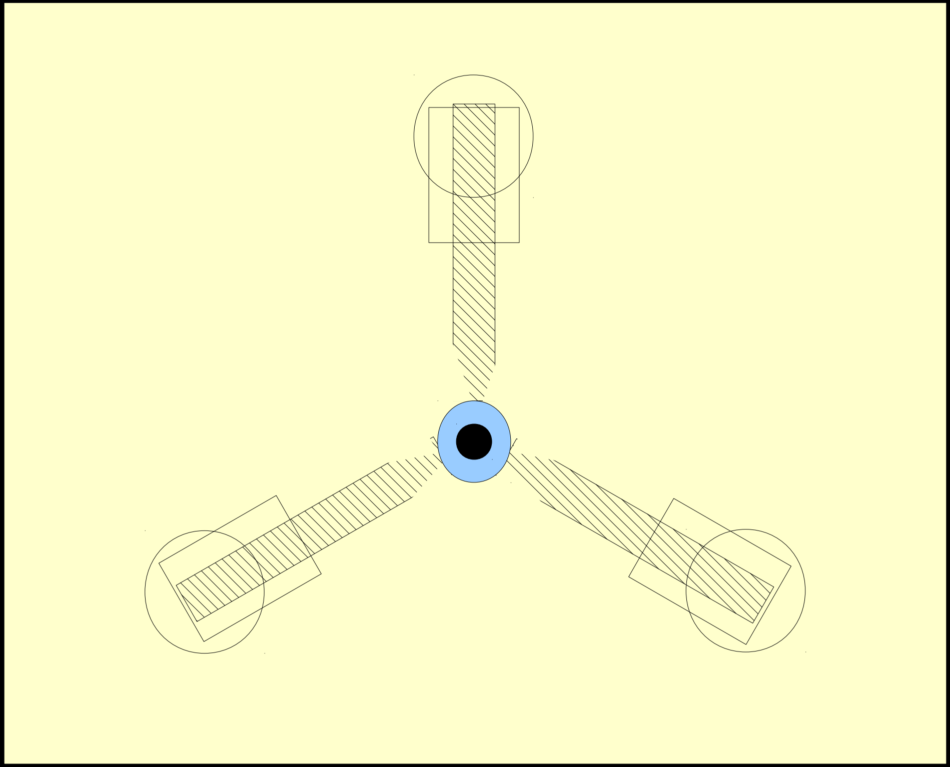
Transporting a watt of waste heat from BEC requires 1.6 gigawatts...

Trouble With Thermodynamics: Keeping it Cool



Transporting a watt of waste heat from BEC requires 1.6 gigawatts...
Even Emmet Brown's flux capacitor only required 1.21 gigawatts!!!

Trouble With Thermodynamics: Keeping it Cool



Transporting a watt of waste heat from BEC requires 1.6 gigawatts...
Even Emmet Brown's flux capacitor only required 1.21 gigawatts!!!
But if the computation is valuable enough, who cares?

What is Quantum Computing's Killer App?

What is Quantum Computing's Killer App?

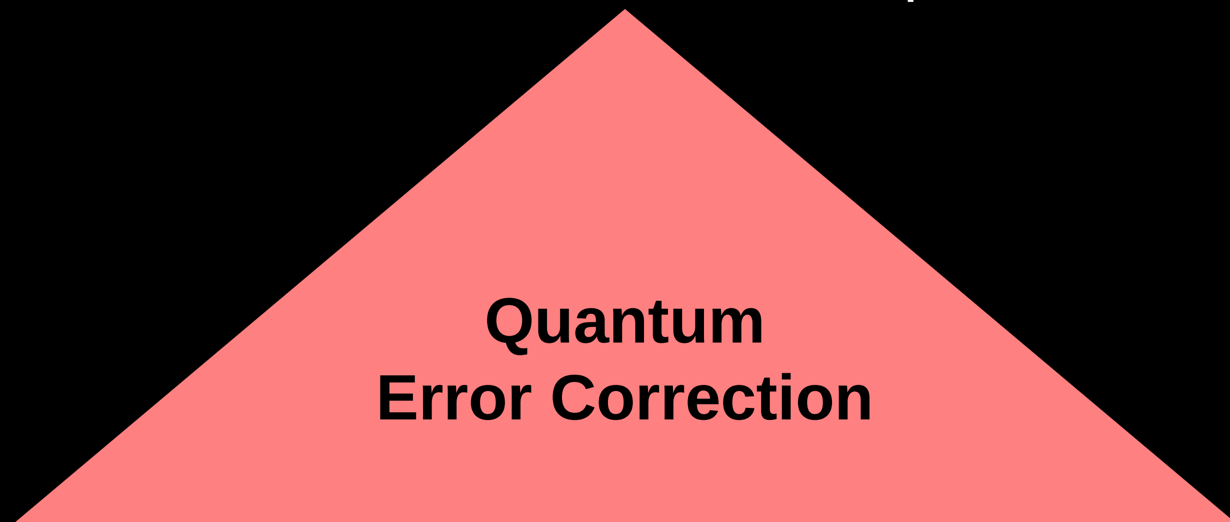
- Current possibilities:
  - Shor's integer factorization algorithm
  - Grover's search algorithm
  - Optimization problems (e.g., traveling salesman problem for logistics)
  - Quantum mechanical dynamics (e.g., quantum chemistry)
  - Gaming

Killer App: Integer Factorization

- Shor's algorithm promises polynomial-time factorization
  - Extremely valuable, if rather destructive
  - Prototyped in 2001: https://arxiv.org/abs/quant-ph/0112176
- Requires general-purpose qubits (IBM-Q, not D-Wave)
  - Thousands of them!
- Assuming 1.4 years per doubling, we have about 15 years until QC cracks 1000-bit RSA
  - Also assumes that Shor's algorithm actually works on real hardware
  - On the other hand, IBM-Q may be adding qubits faster than 1.4 years per doubling, doubling every 8 months from May 2016 to May 2017
  - So it might not be too early to start work on QC-resistant cyphers!!!

Killer App: Integer Factorization: Quantum Error Rate

“A few thousand” stable qubits



One hundred million real qubits

https://spectrum.ieee.org/computing/hardware/google-plans-to-demonstrate-the-supremacy-of-quantum-computing

Killer App: Integer Factorization: Quantum Error Rate

“A few thousand” stable qubits

Quantum Error Correction

One hundred million real qubits

15-30 years, so still not to early for QC-resistant cypher!!!
But I/O and error rates might add another 15 years...

https://spectrum.ieee.org/computing/hardware/google-plans-to-demonstrate-the-supremacy-of-quantum-computing

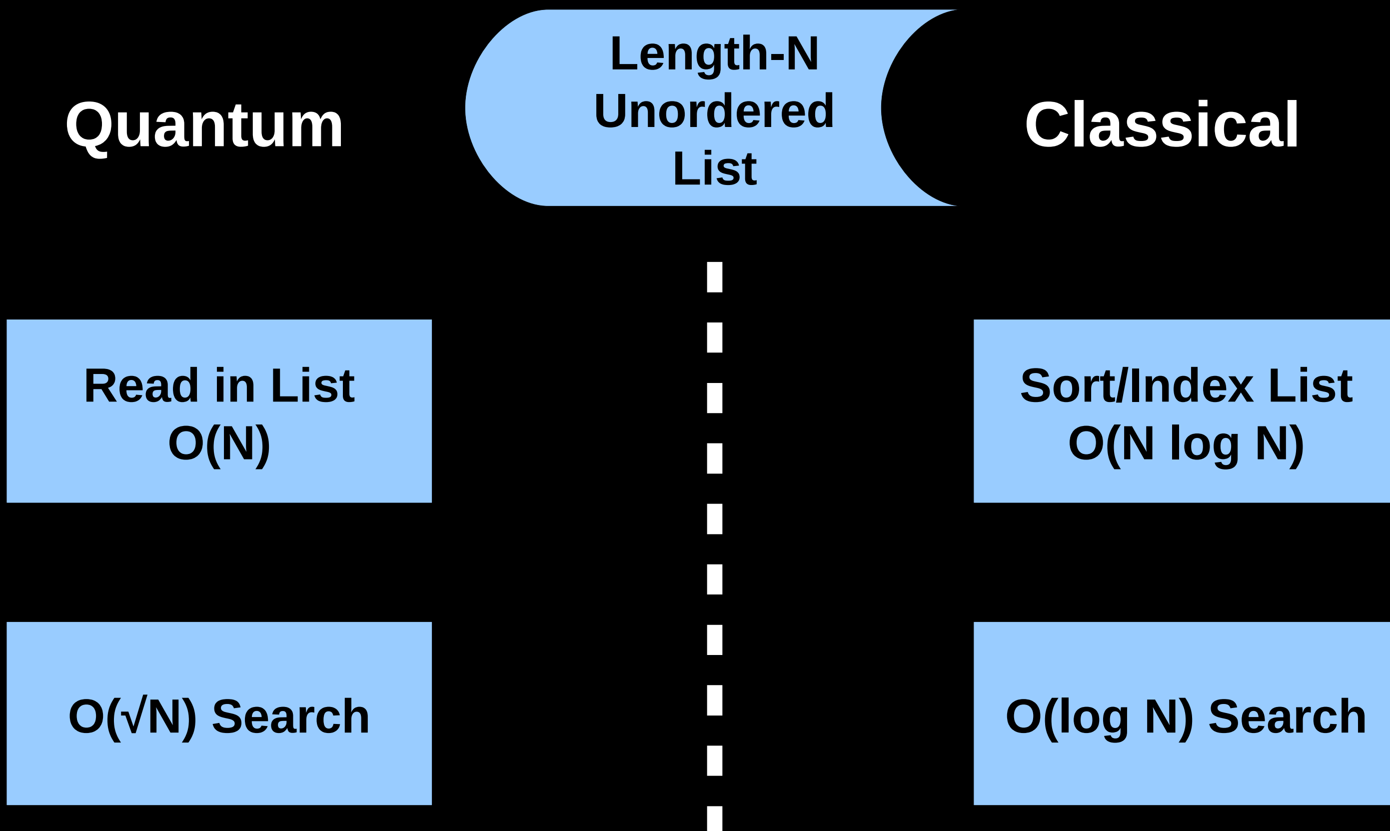
Killer App: Integer Factorization: Competition

- 2002: Polynomial-time integer primality test
- Perhaps integer factorization will also succumb to pure math
  - Easy to dismiss this unless you review the past 50 years of progress:
    - 1970: Proof that Hilbert's 10th problem is unsolvable
    - 1976: Proof of the four-color problem (stood for centuries)
    - 1984: Polynomial-time algorithm for solving linear programming problems
    - 1994: Proof of Fermat's Last Theorem (stood for centuries)
    - 1998: Proof of Kepler's conjecture (sphere packing, stood for centuries)
    - 2002: Proof of Catalan's conjecture (2^3 and 3^2, stood for centuries)
    - 2003: Proof of the Poincaré conjecture (topology)
    - 2004: Proof of the classification of finite simple groups
    - 2013: Proof that there is no bound on the values of pairs of primes differing by a finite number (first real progress in more than **two millennia**)

Killer App: Integer Factorization: Competition

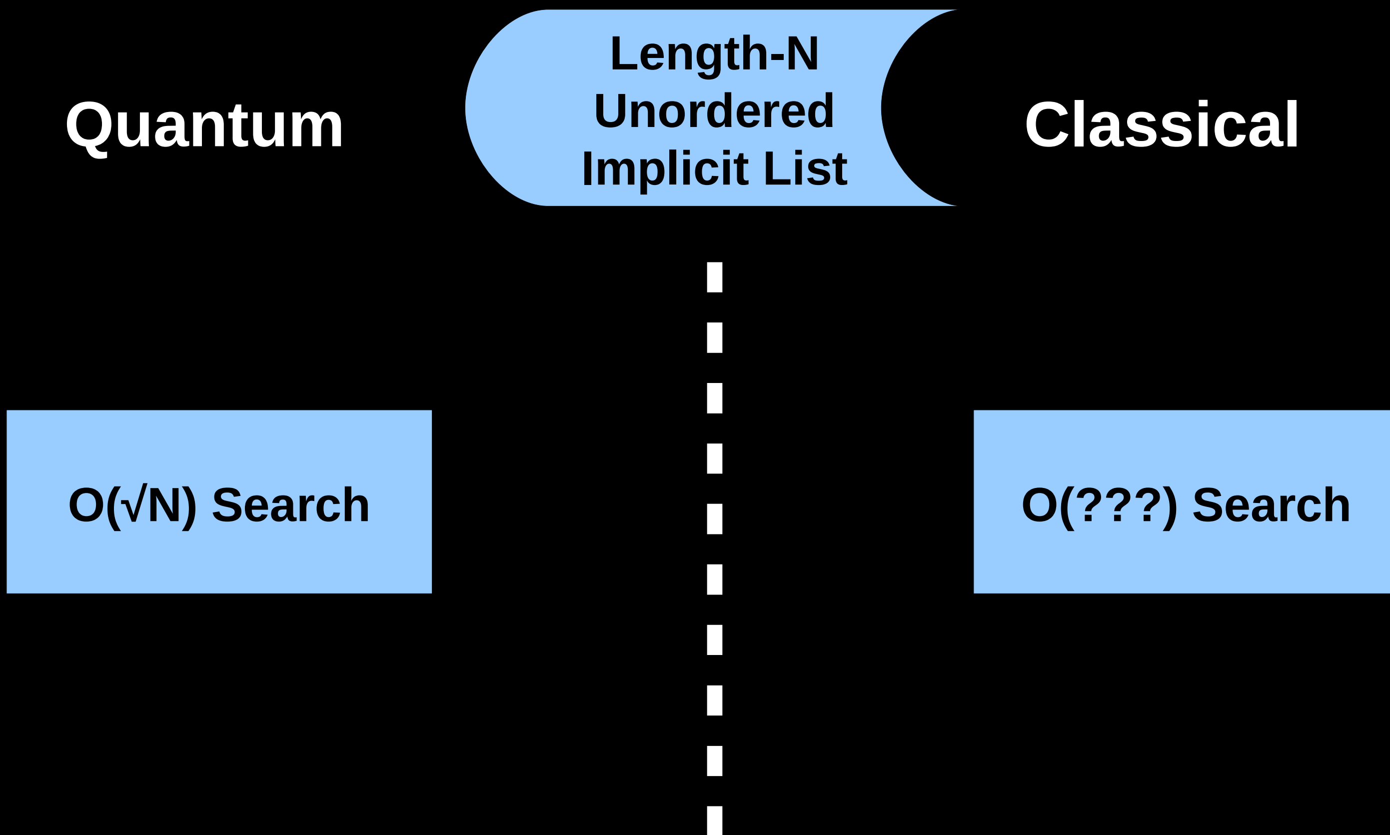
- 2002: Polynomial-time integer primality test
- Perhaps integer factorization will also succumb to pure math
  - Easy to dismiss this unless you review the past 50 years of progress:
    - 1970: Proof that Hilbert's 10th problem is unsolvable
    - 1976: Proof of the four-color problem (stood for centuries)
    - 1984: Polynomial-time algorithm for solving linear programming problems
    - 1994: Proof of Fermat's Last Theorem (stood for centuries)
    - 1998: Proof of Kepler's conjecture (sphere packing, stood for centuries)
    - 2002: Proof of Catalan's conjecture (2^3 and 3^2, stood for centuries)
    - 2003: Proof of the Poincaré conjecture (topology)
    - 2004: Proof of the classification of finite simple groups
    - 2013: Proof that there is no bound on the values of pairs of primes differing by a finite number (first real progress in more than **two millennia**)
- So QC needs to step lively if it wants this one!

Killer App: Grover's Search Algorithm for DBMS: Search Length-N Unordered List in O(√N) Time



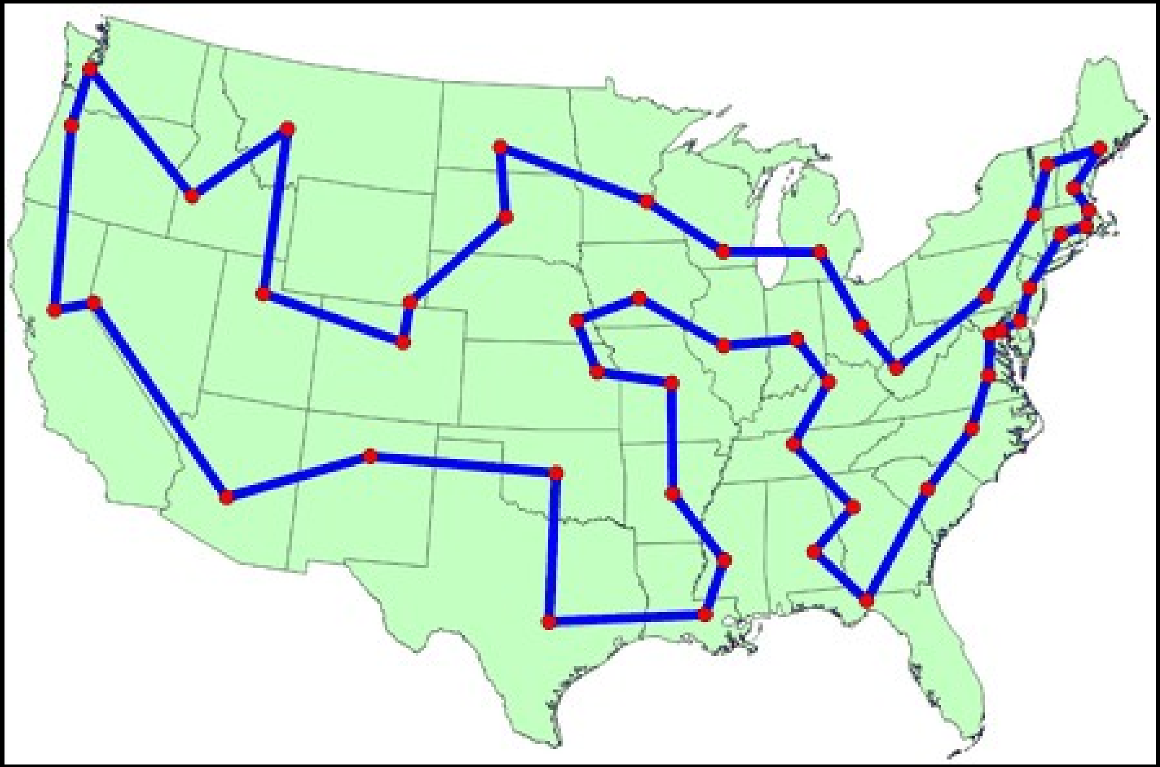
When there are sufficient searches, classical computing wins

Killer App: Grover's Algorithm Remaining Hope: Cases Where List is Implicit, Need Not Be Formed



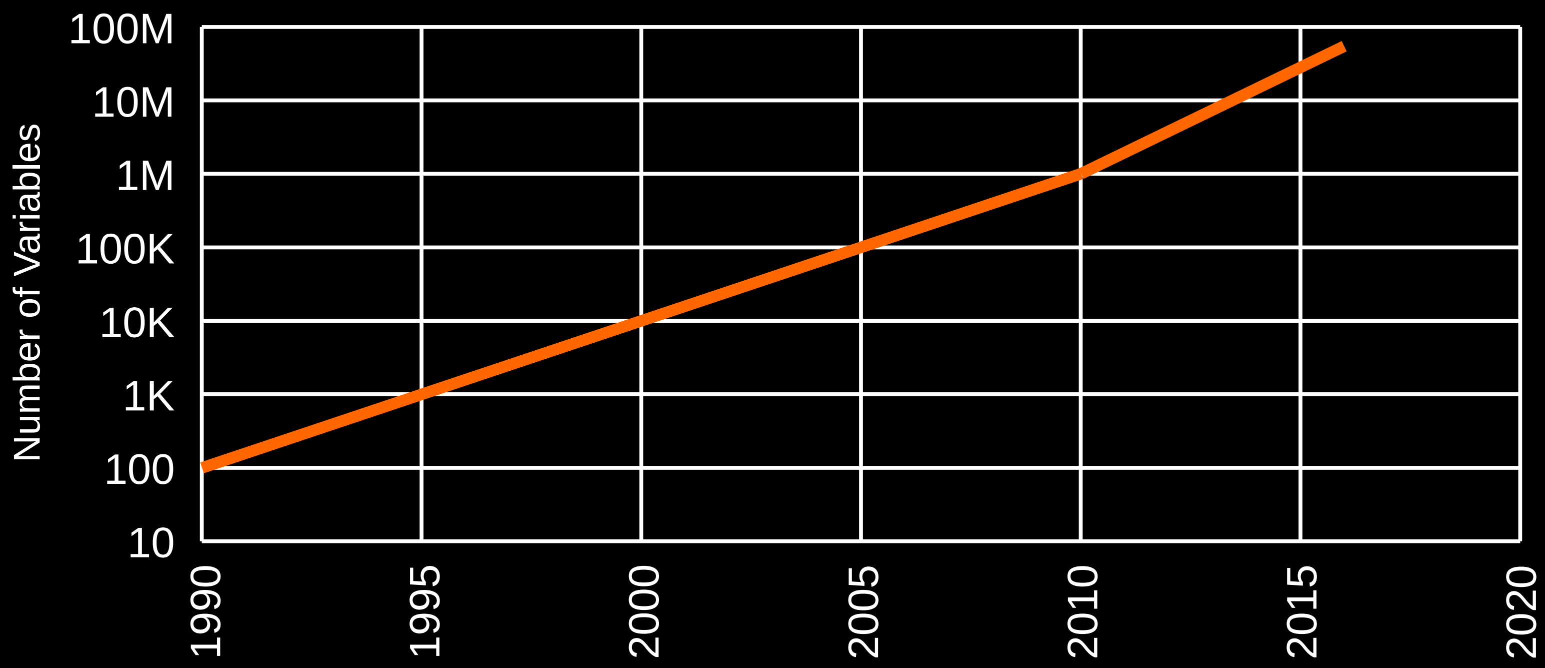
Searching for factors of a large composite number is one example

Killer App: Traveling Salesman Problem (TSP)



Polynomial-time algorithm guaranteed within 40% of optimal solution
2006 solvers finding optimal solutions to 85,900-city problems
Seven years for D-Wave to catch up, assuming one qubit per city and no classical-computing progress

Killer App: Boolean Satisfiability (SAT) Problem

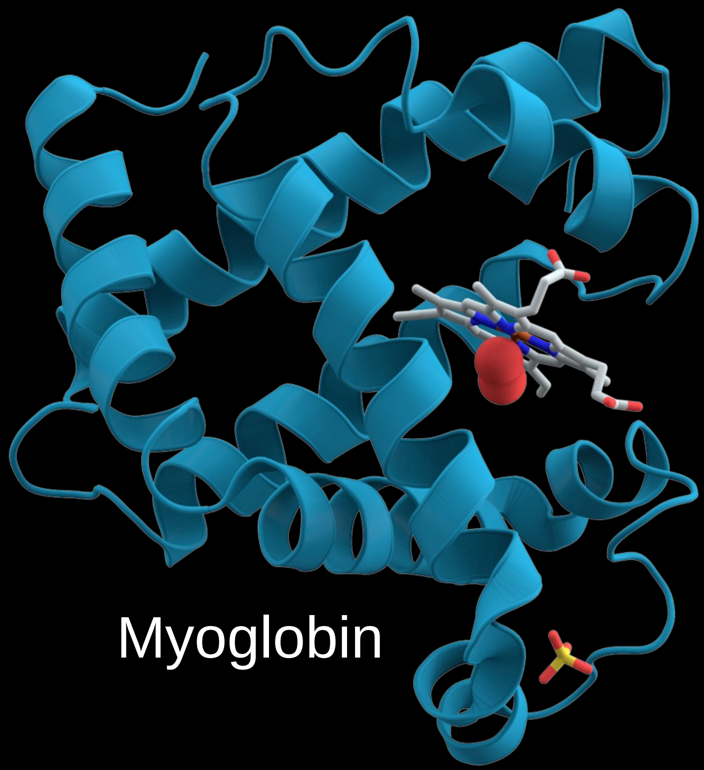


SAT is NP-complete, but heuristics' capabilities doubling about every 1.3 years
Early experiments incorporating machine learning showing some promise
Classical computing is putting up an impressive fight!!!

Killer App: Solving Other Optimization Problems

- To be fair, TSP and SAT have received huge investments
  - Classical computing thus has a huge head start
  - Machine learning also likely to help in near term
- Perhaps less well-known problem become important
  - And provide QC with a level playing field
  - One possible current example: SAT involving pigeonhole principle
- To probe deeper:
  - https://en.wikipedia.org/wiki/Quantum_algorithm
  - http://www.epsnews.eu/2017/04/quantum-computers-for-exponentially-hard-problems/
  - https://arxiv.org/abs/1801.00862

Killer App: Quantum Mechanical Dynamics (QMD)



Myoglobin

Consumes entire clusters inverting billion-row/column sparse matrices

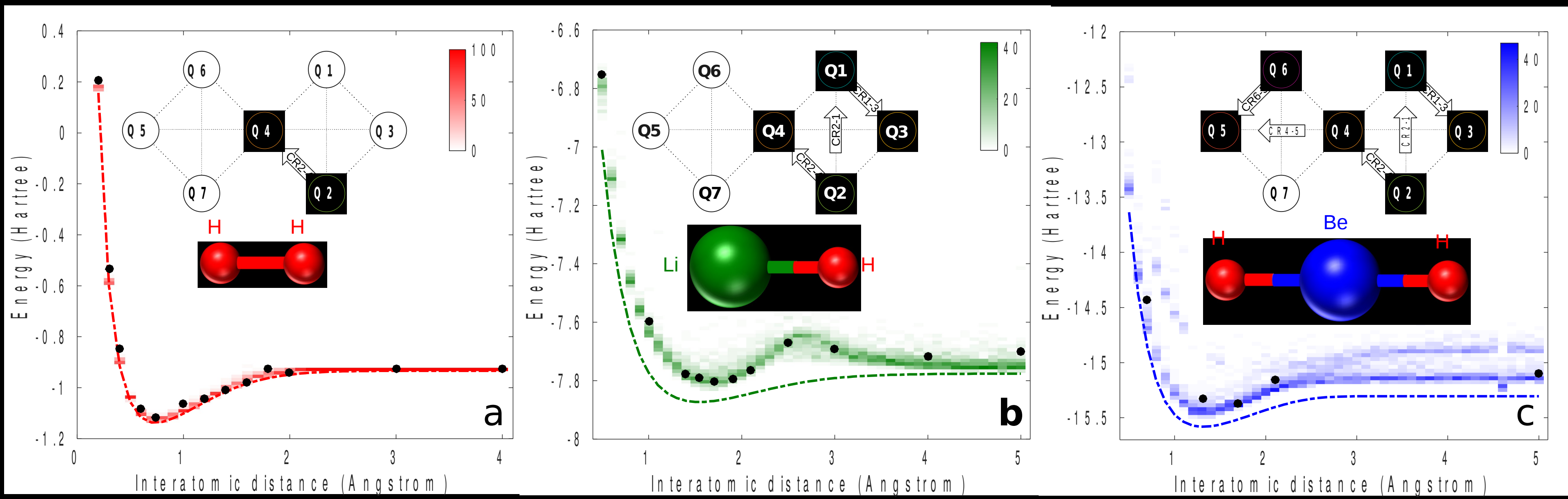
IBM, Microsoft, Harvard interested, IBM looking to 50-qubit PoC

H_2, LiH, BeH_2 thus far (https://arxiv.org/abs/1704.05018)

Chinese researchers looking to QC for quantum photon modeling

Competition: fold.it, machine learning, advances in physical chemistry

Killer App: Quantum Mechanical Dynamics (QMD)

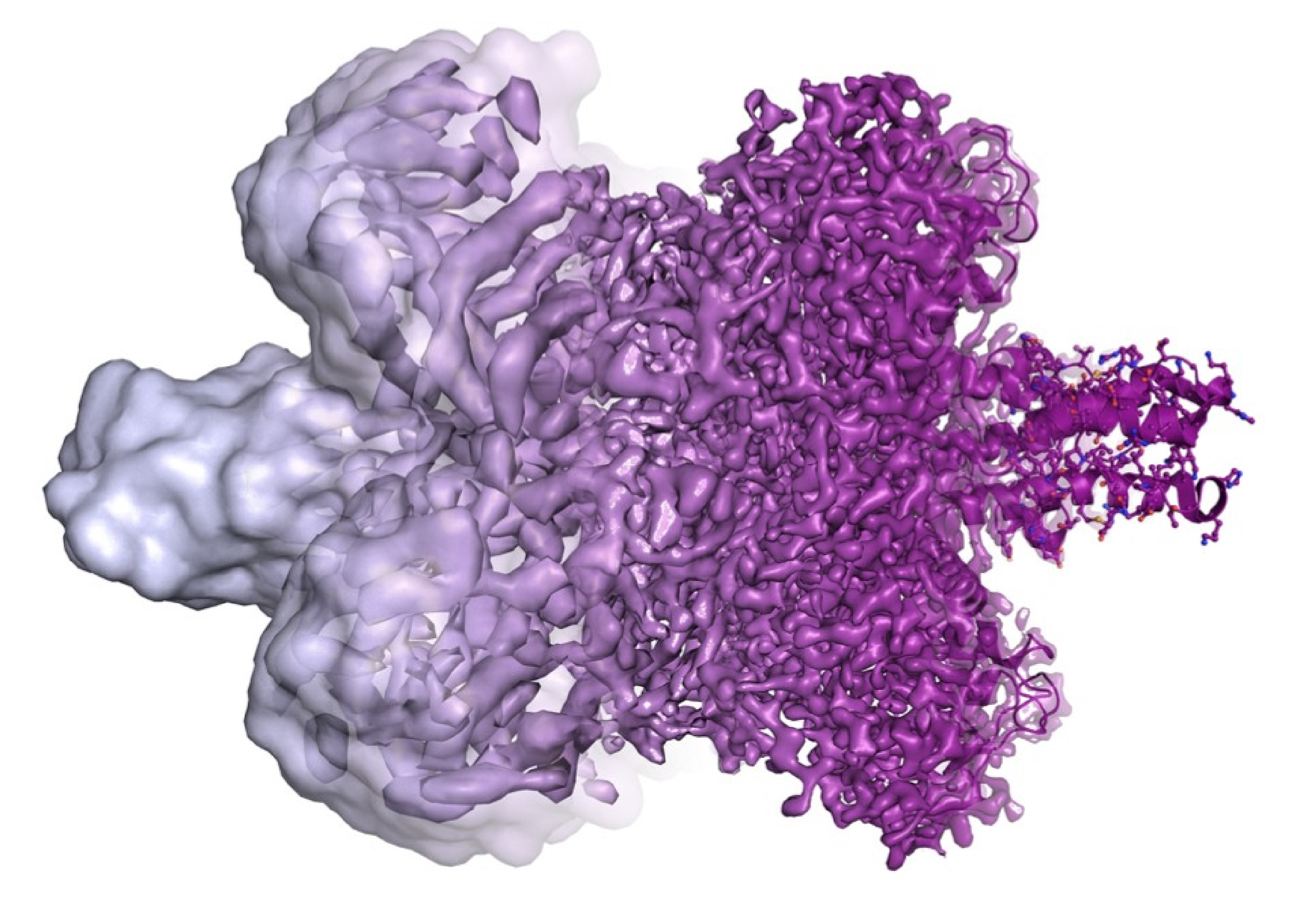


IBM used up to six qubits of its superconducting quantum processor to address electronic structure problems for the molecules H_2, LiH and BeH_2

50-qubit system performance/scalability PoC planned

A. Kandala, A. Mezzacapo, K. Temme, M. Takita, M. Brink, J. M. Chow, J. M. Gambetta, arXiv 1704.0518, Nature (2017, in press embargo)

Advance in Physical Chemistry



2017 Nobel Prize in Chemistry: Joachim Frank, Richard Henderson, Jacques Dubochet

https://arstechnica.com/science/2017/10/algorithm-designer-among-those-honored-with-the-chemistry-nobel/

IBM

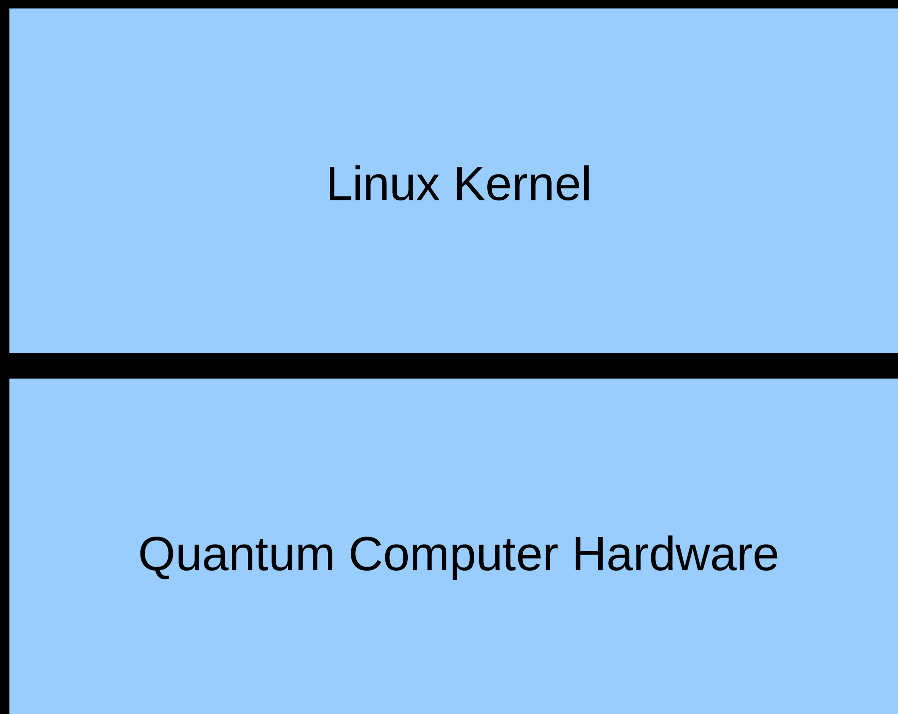
Killer App: Gaming???

```
We start with Player 1.
Look away Player 2!

The lines in the bowtie shape below are the places you can place your ship.

|\     /|
| d   b |
|  \ /  |
f   X   a
|  / \  |
| e   c |
|/     \|


Choose a line for your ship. (a, b, c, d, e or f)


Player 2: You're up!
```

https://medium.com/@decodoku/quantum-battleships-the-first-multiplayer-game-for-a-quantum-computer-e4d600ccb3f3

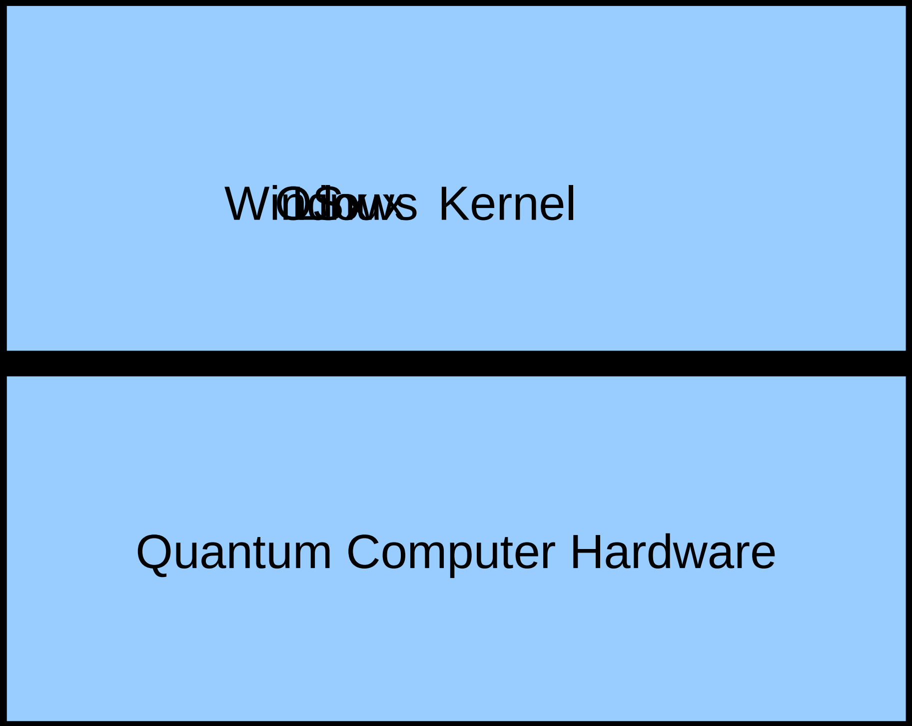
Quantum Computing and Linux?

Quantum Computing and Linux?

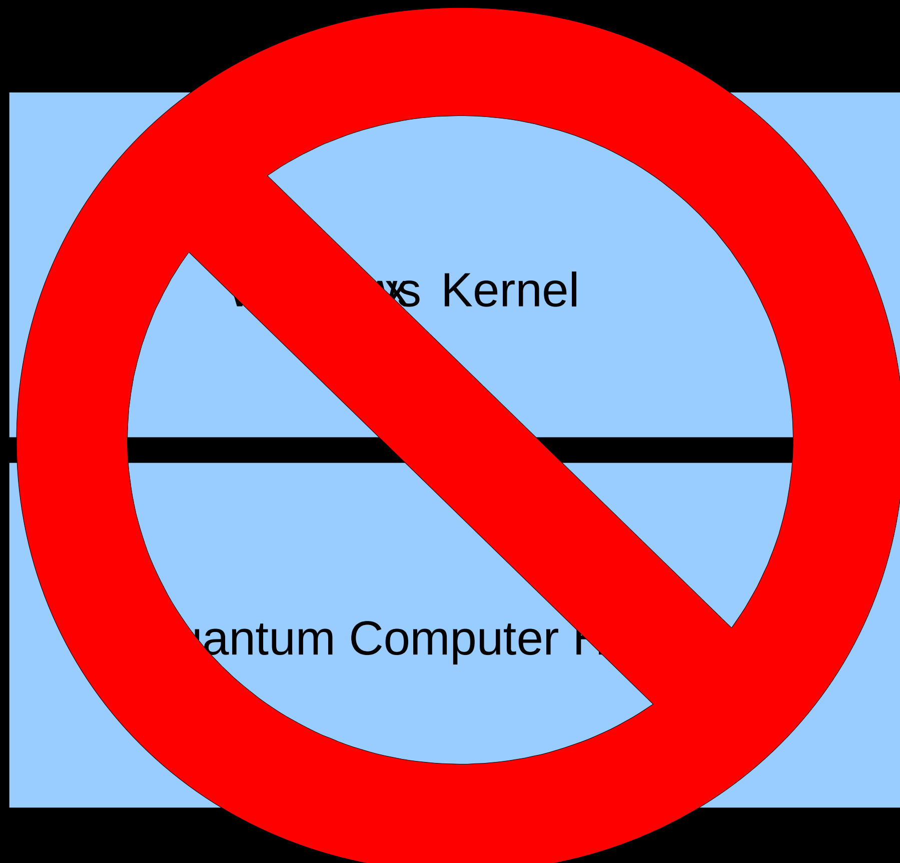


But this is quantum computing!!!

Quantum Computing: Why not Superposed OSes?

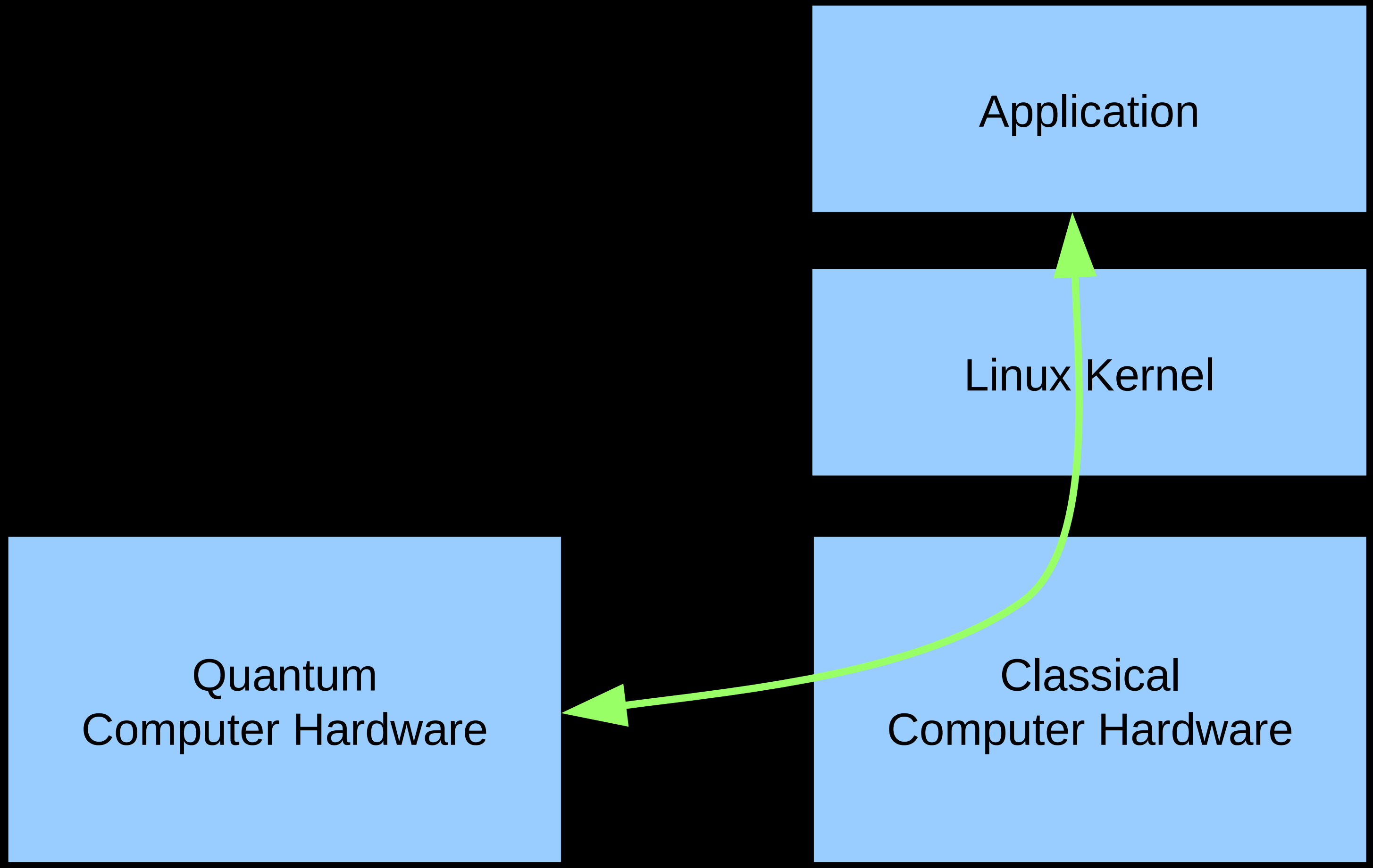


Quantum Computing: Why not Superposed OSes?



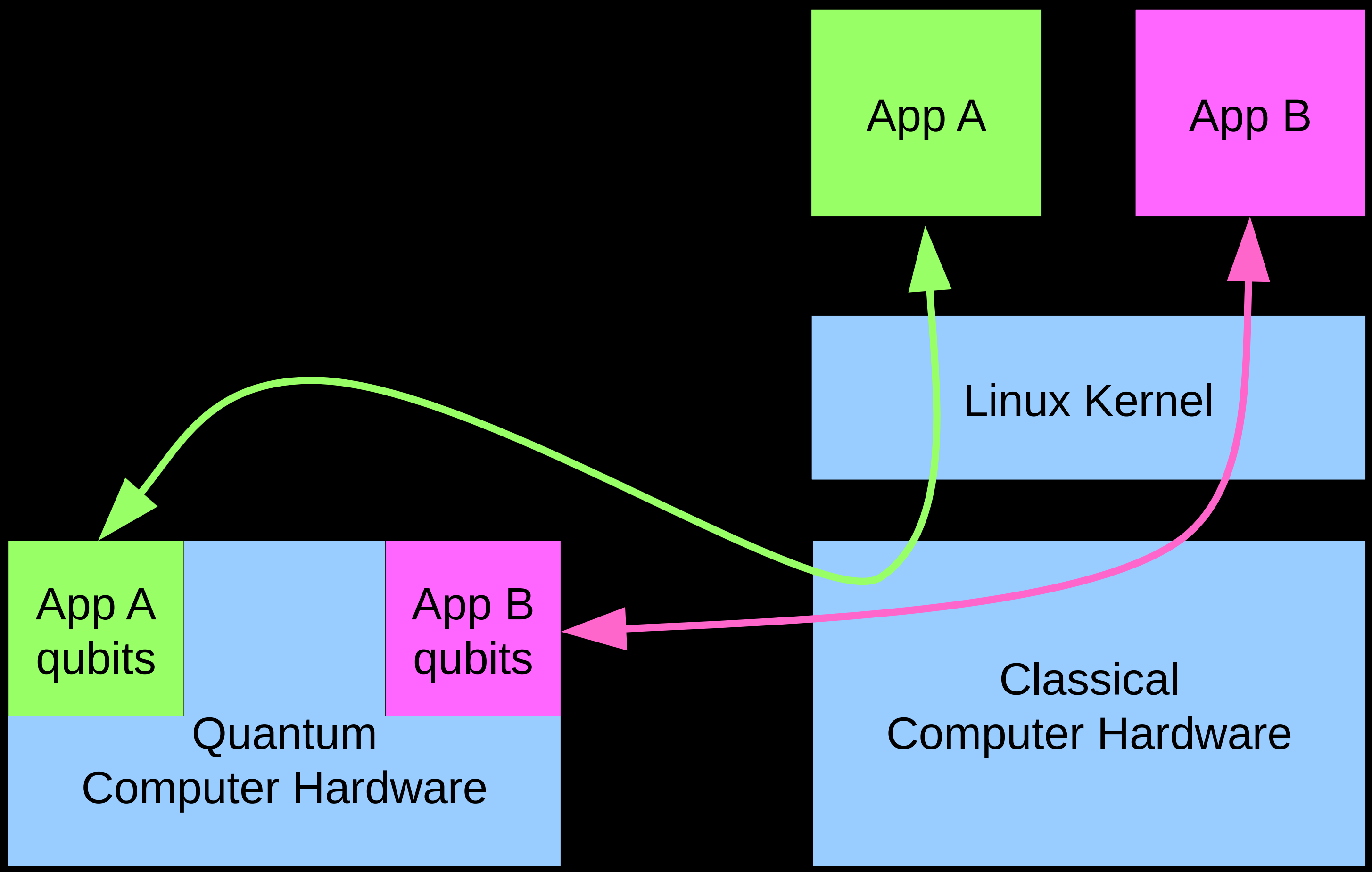
Not without a **lot** more qubits!!!

Quantum Computing and Linux?



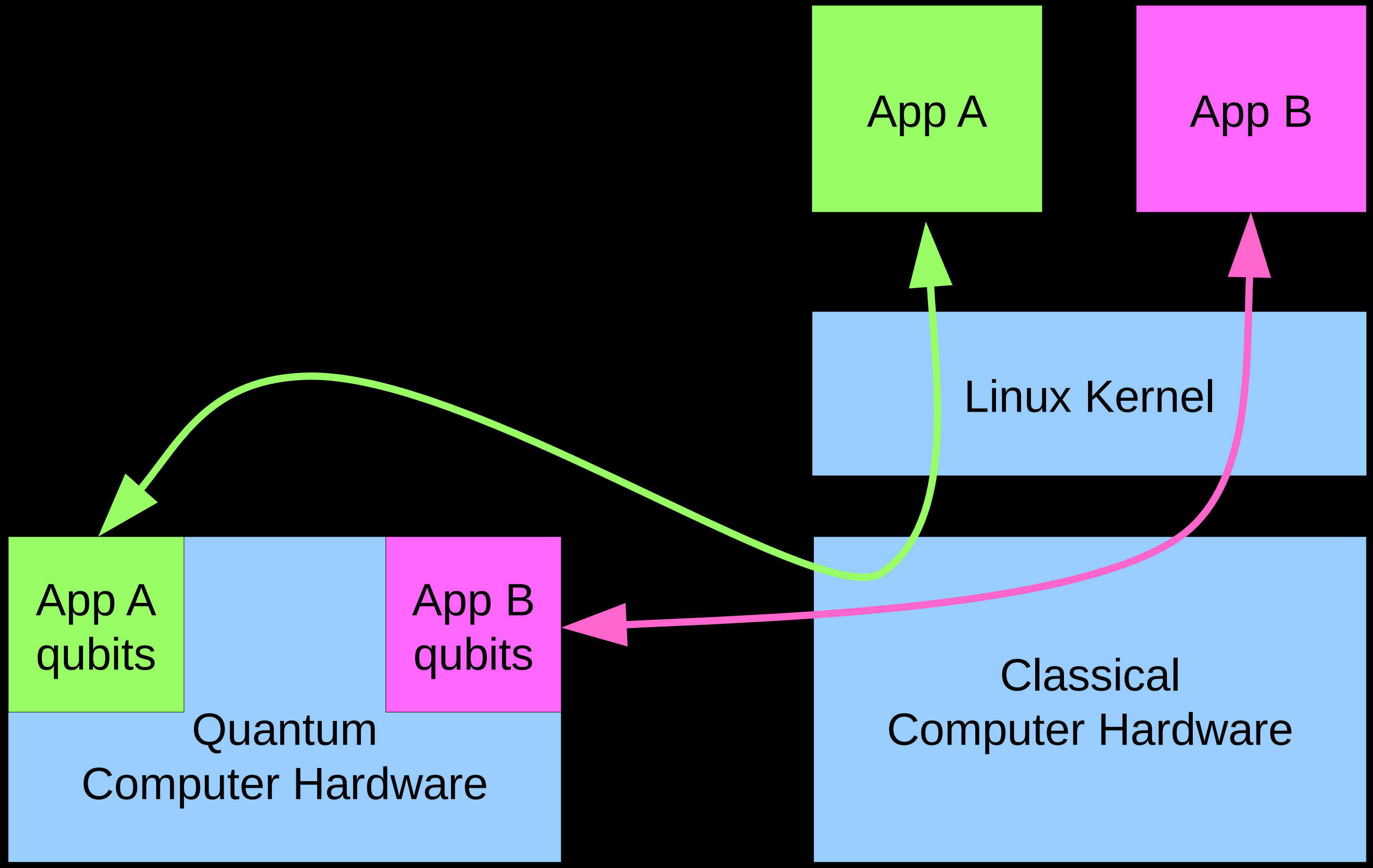
Accelerator, similar to GPGPU or FPGA
But no context switching, at least not until quantum memory

Quantum Computing and Linux?



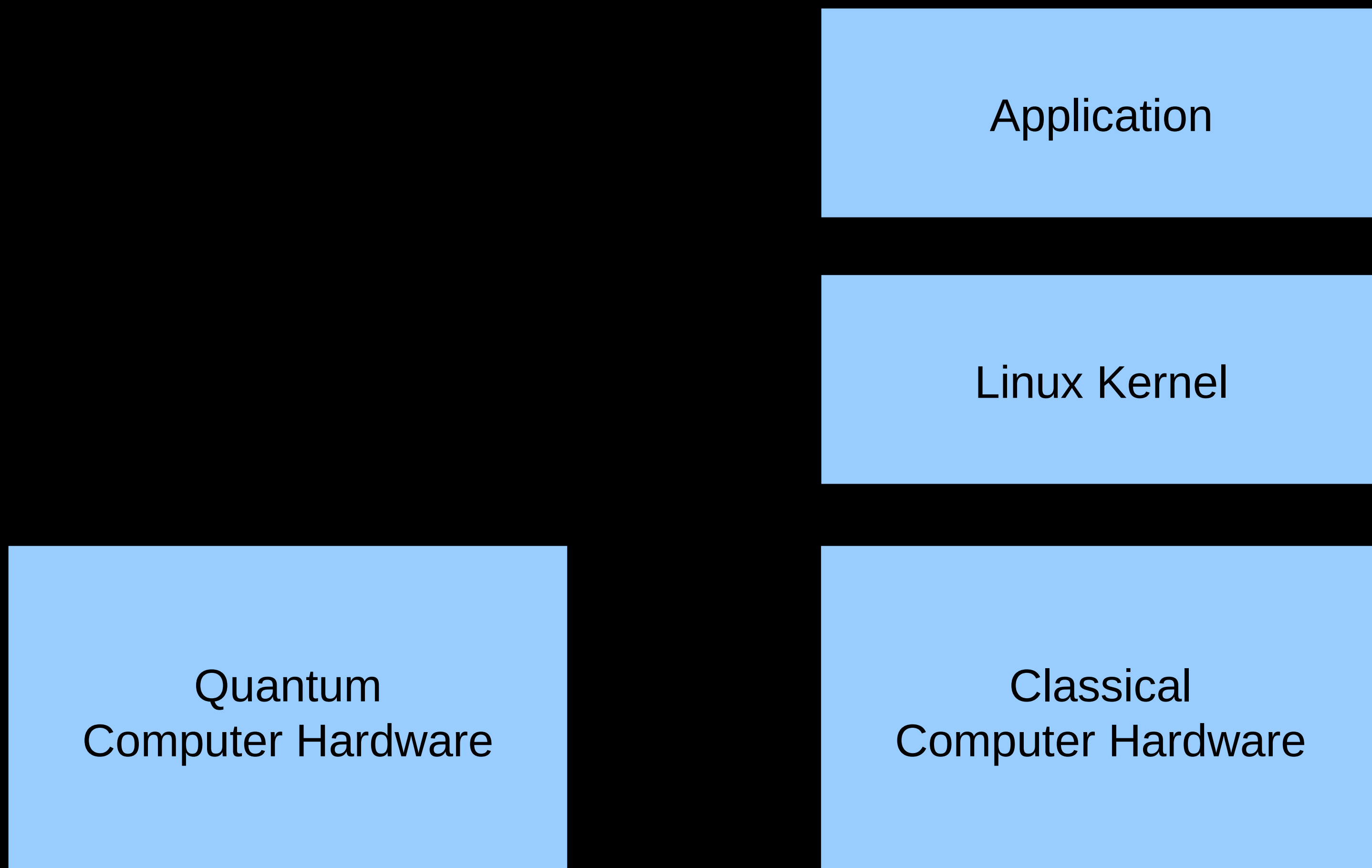
Maybe qubit-division multiplexing? Isolation? Security? Quantum Meltdown/Spectre?

Quantum Computing and Linux?

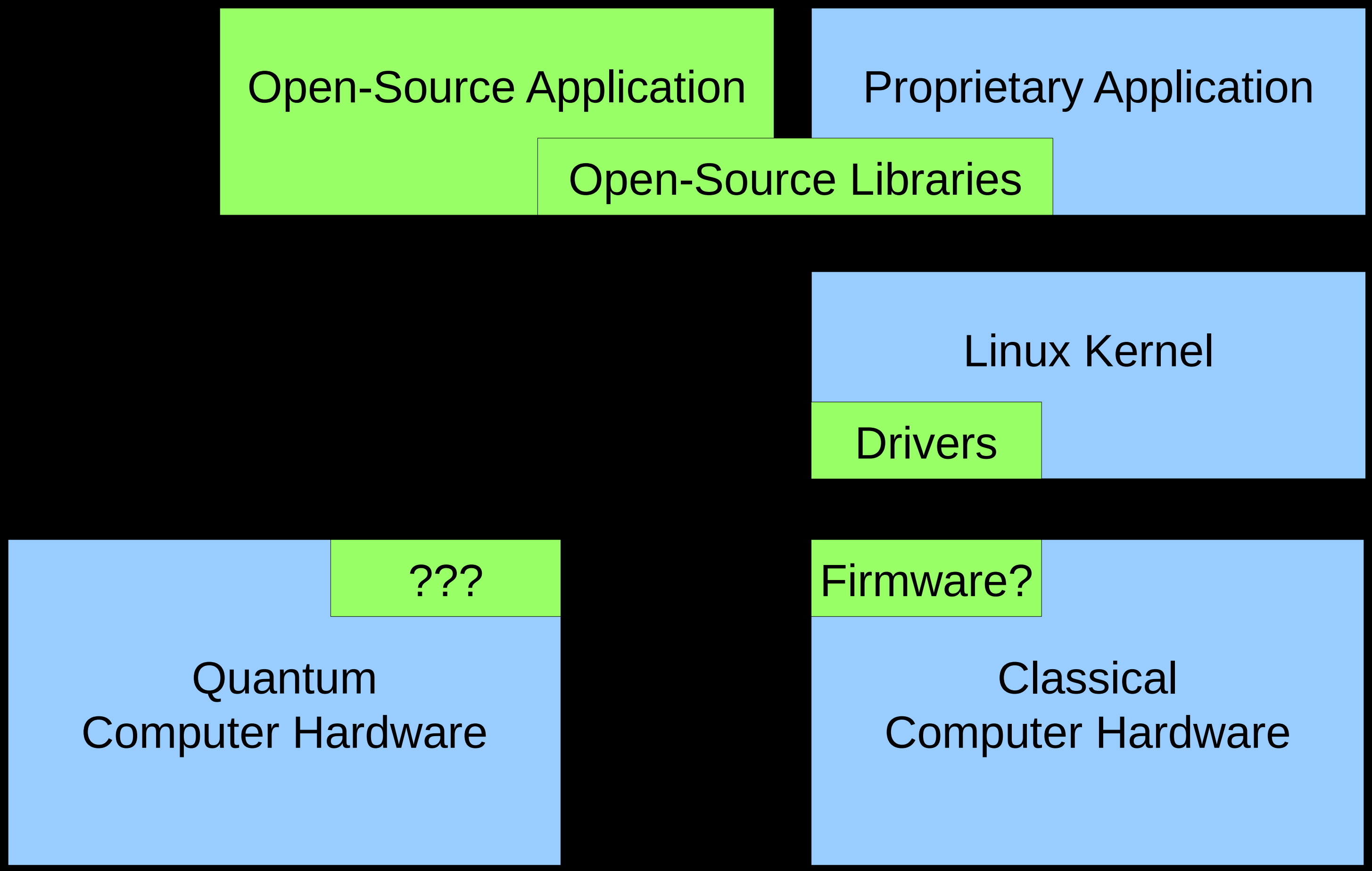


Maybe qubit-division multiplexing? Isolation? Security? Quantum Meltdown/Spectre?
Need quite a few more qubits before this is a real problem!!!

Quantum Computing and Open Source???



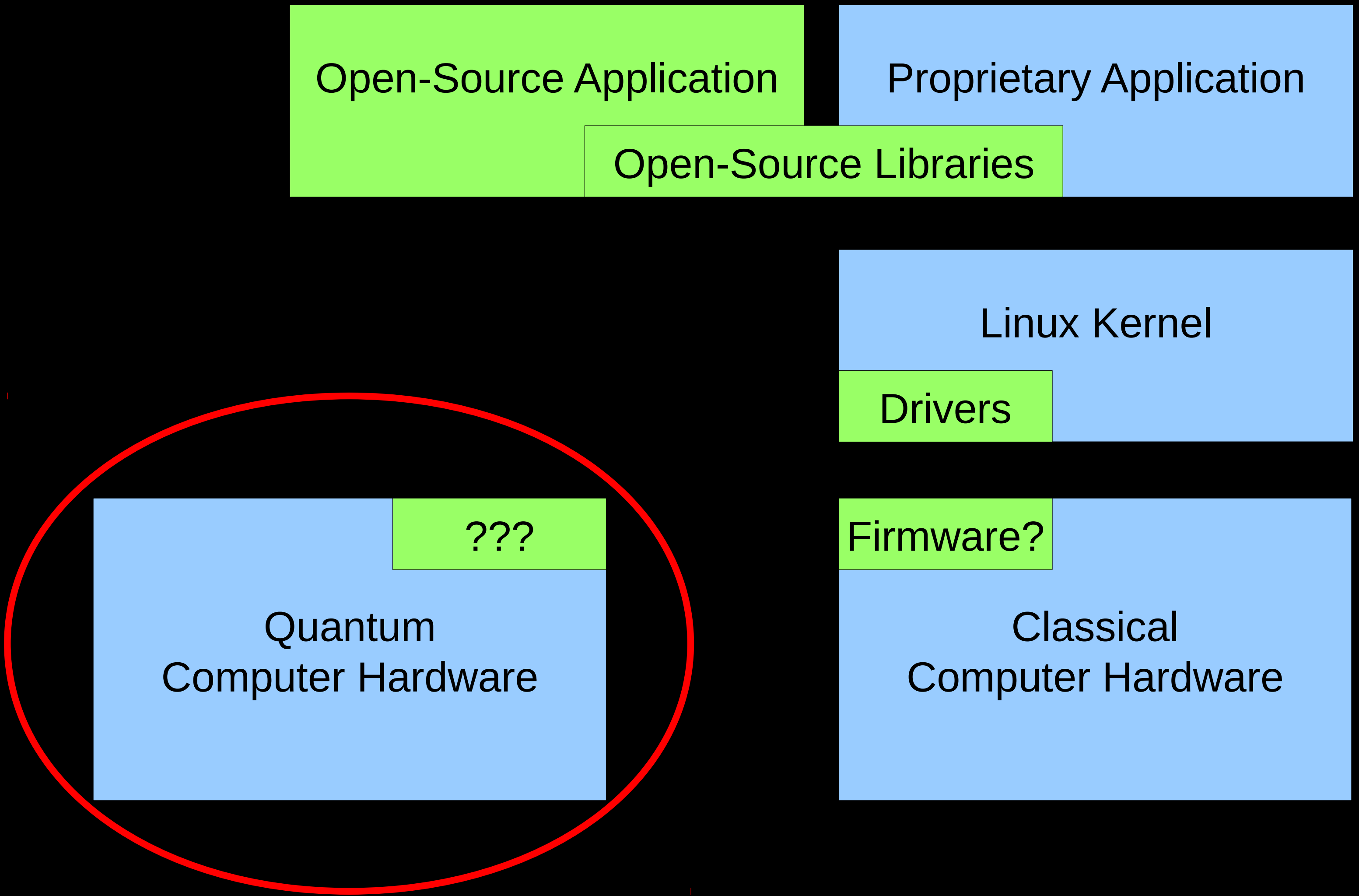
Quantum Computing and Open Source???



We should expect the collaboration to continue!!!

IBM

Quantum Computing and Open Source???



We should expect the collaboration to continue!!!

Quantum Computing Hardware and Open Source???

Quantum Computing Hardware and Open Source???

Need Small Low-Power Precise Signal Generators

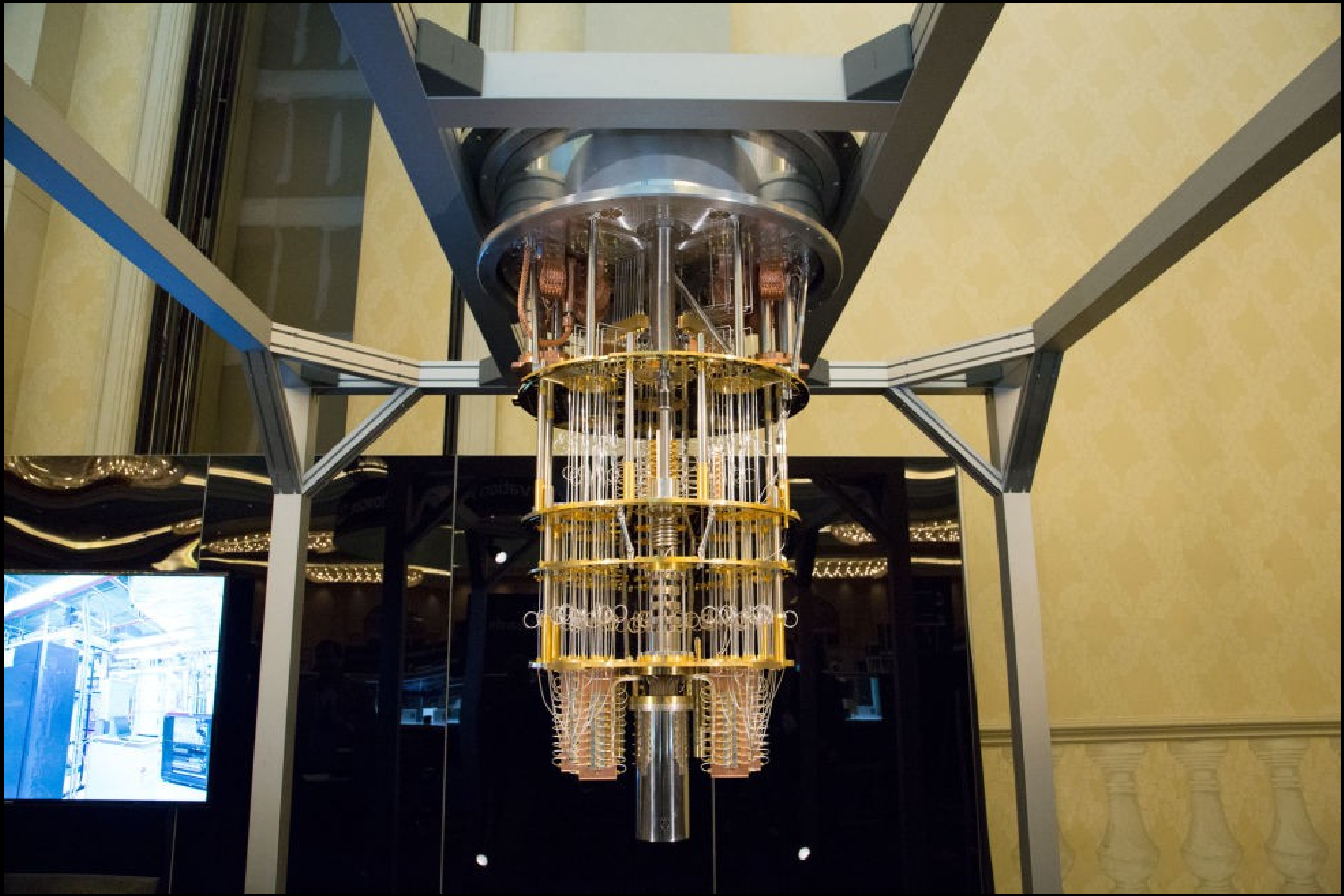
$N@C_{60}$

Need Small Low-Power Precise Signal Generators

$$N@C_{60}$$

Considered for nano-scale atomic clocks.
Yours for only $167M per gram!!!
Many other candidates for nano-scale signal generators.

Quantum Computing Hardware and Open Source???



Summary

Summary

- Within past decade, QC moved from theory to real hardware
  - Quantum error rates are currently the limiting factor
- QC will be accelerator, shared by partitioning
  - We won't be running Linux on QC itself, not anytime soon, anyway
  - But a great deal of open-source software will surround QC
- QC needs killer app: Some possibilities, but jury still out
  - Optimization and quantum mechanical dynamics current best bets
  - Note: Quantum cryptography already seeing some use
- Classical computing is putting up quite a fight!!!
  - Competition should be good for end users no matter who wins
- Free advice:
  - If you can afford it, do both classical and quantum computing
  - If you can only afford one, stick with classical computing

Summary

- Within past decade, QC moved from theory to real hardware
  - Quantum error rates are currently the limiting factor
- QC will be accelerator, shared by partitioning
  - We won't be running Linux on QC itself, not anytime soon, anyway
  - But a great deal of open-source software will surround QC
- QC needs killer app: Some possibilities, but jury still out
  - Optimization and quantum mechanical dynamics current best bets
  - Note: Quantum cryptography already seeing some use
- Classical computing is putting up quite a fight!!!
  - Competition should be good for end users no matter who wins
- Free advice:
  - If you can afford it, do both classical and quantum computing
  - If you can only afford one, stick with classical computing
  - Disclaimer: This advice is subject to change without notice

Legal Statement

- This work represents the view of the author and does not necessarily represent the view of IBM.
- IBM and IBM (logo) are trademarks or registered trademarks of International Business Machines Corporation in the United States and/or other countries.
- Linux is a registered trademark of Linus Torvalds.
- Other company, product, and service names may be trademarks or service marks of others.

Questions?