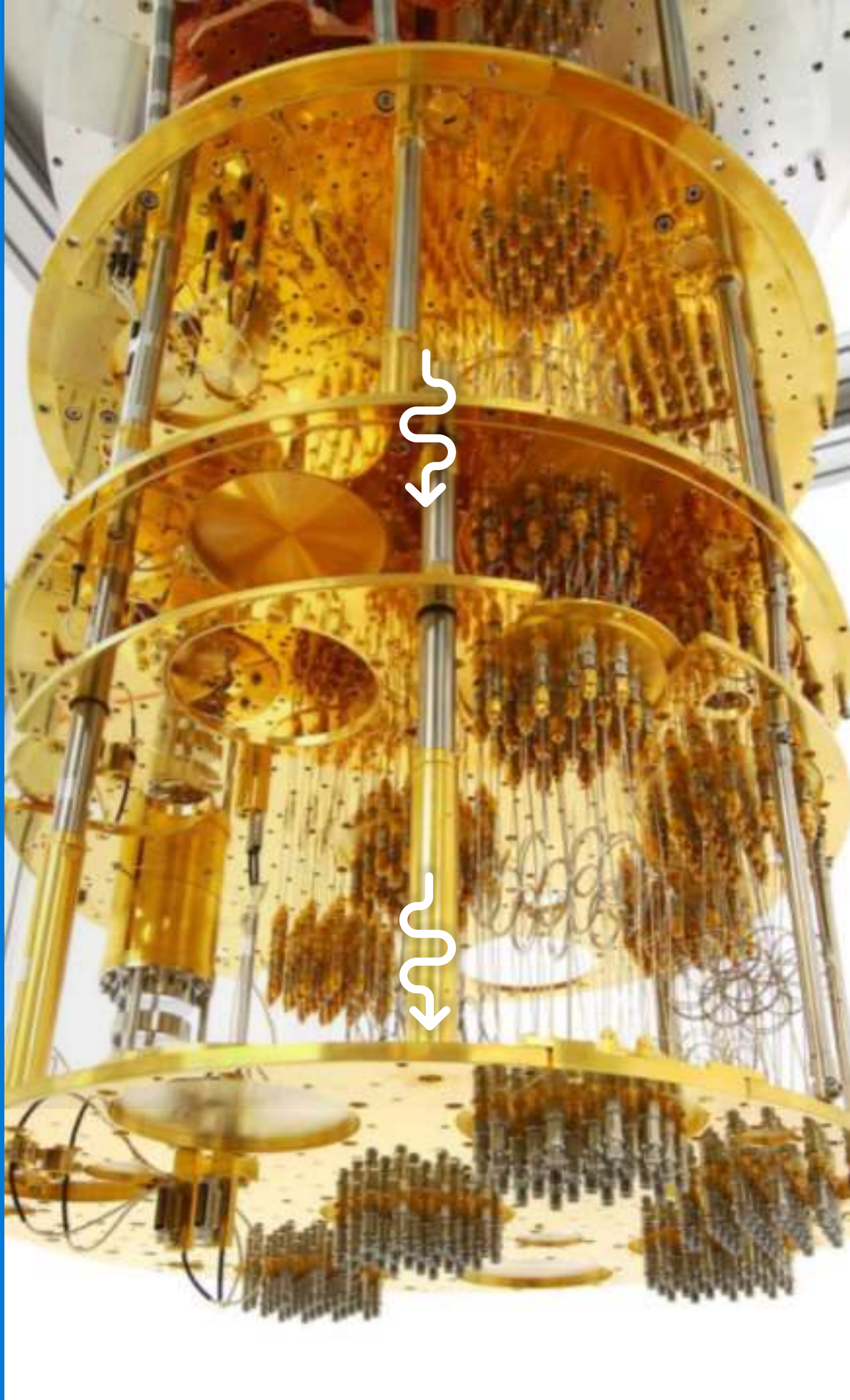
Microsoft

High Performance Quantum Computing

Prof. Matthias Troyer
Principal Researcher



Cray X-MP/28 at ETH Zurich in 1988

Beyond exascale computing

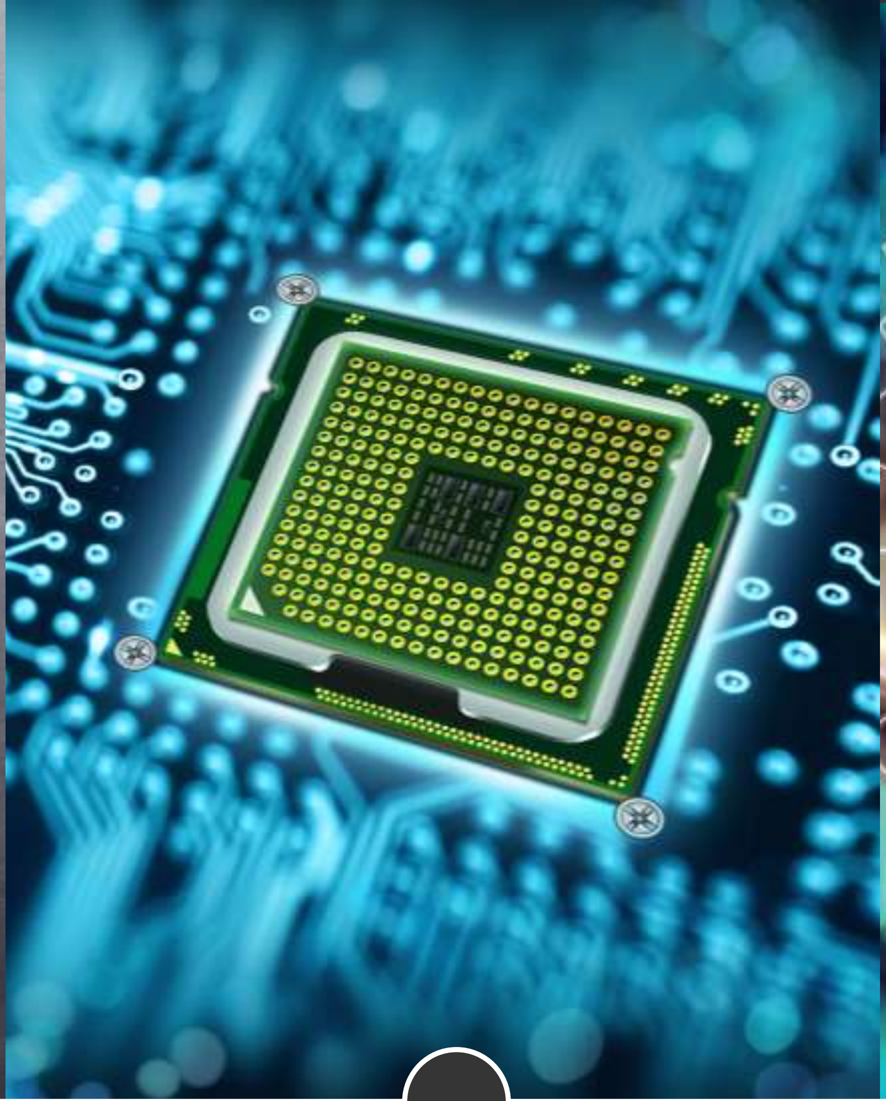
Argonne NATIONAL LABORATORY

Enabling technologies for beyond exascale computing

- We are not referring to 10**21 flops
- "Beyond exascale" systems as we are defining them will be based on new technologies that will finally result in the much anticipated (but unknown) phase change to truly new paradigms/methodologies.

Paul Messina
Director of Science
Argonne Leadership Computing Facility
Argonne National Laboratory

July 9, 2014
Cetraro



2500
BC

20th
Century

21st
Century

Addressing classically intractable problems

Classical	Quantum
1 billion years	100 seconds

Impact on Cryptography

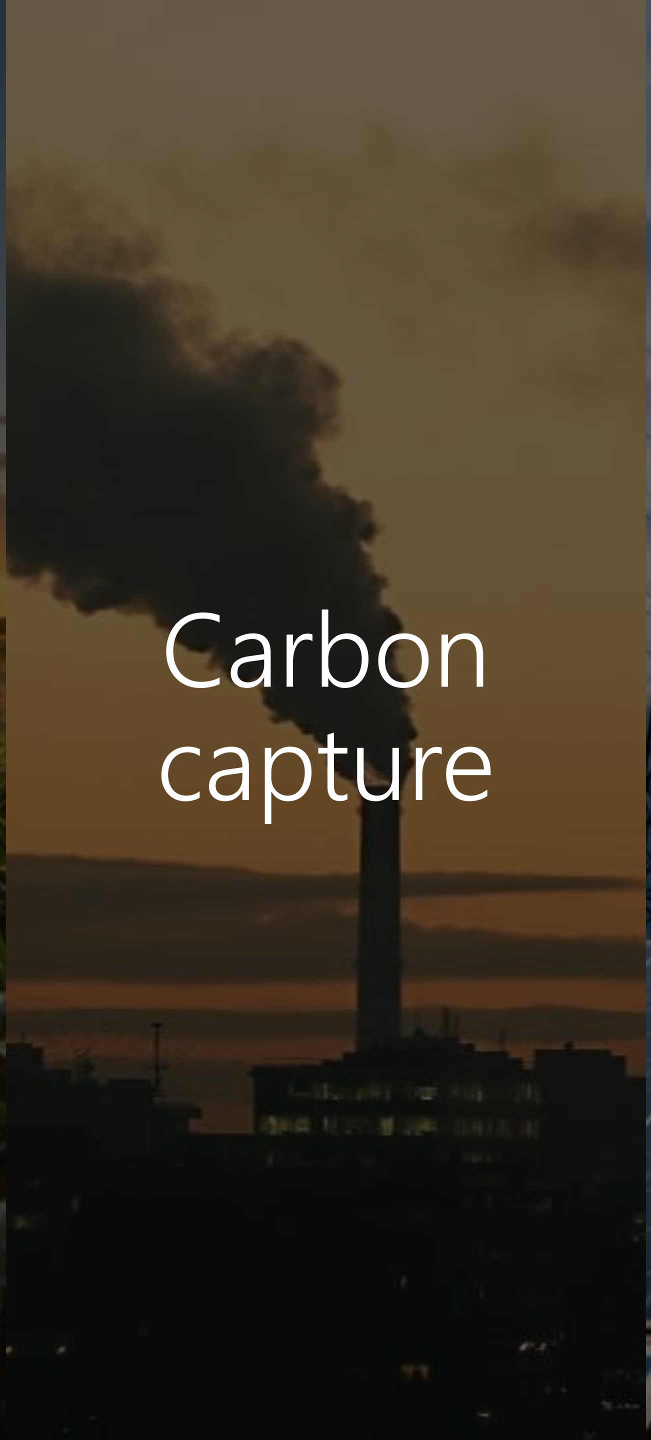
Quantum computers break widely used public key encryption

- RSA-2048 with 4100 qubits
- ECC: Bitcoin with 2330 qubits

New quantum-safe cryptography

- Quantum key distribution
- “Post-quantum” classical cryptography research at Microsoft

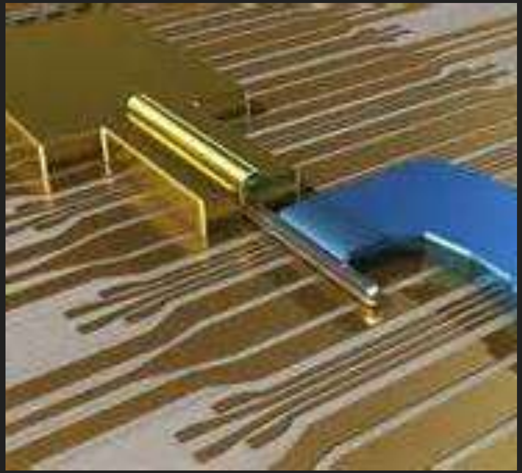

Nitrogen fixation

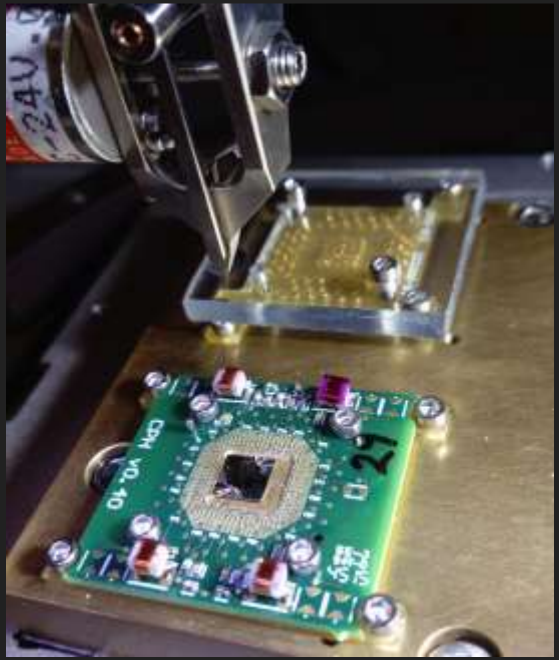

Carbon capture


Materials science


Machine learning

Develop and deploy a scalable, commercial quantum system to solve today’s unsolvable problems





2018

Microsoft's Unique Approach

Revolutionary topological approach

A global team

Scalable, end-to-end technology

Redmond

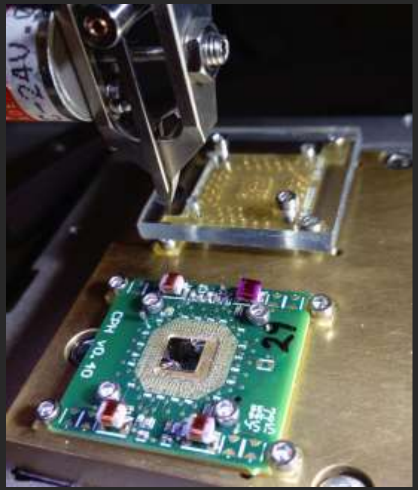
Santa Barbara

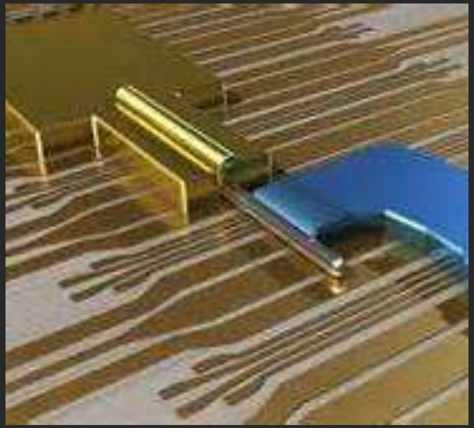
Delft

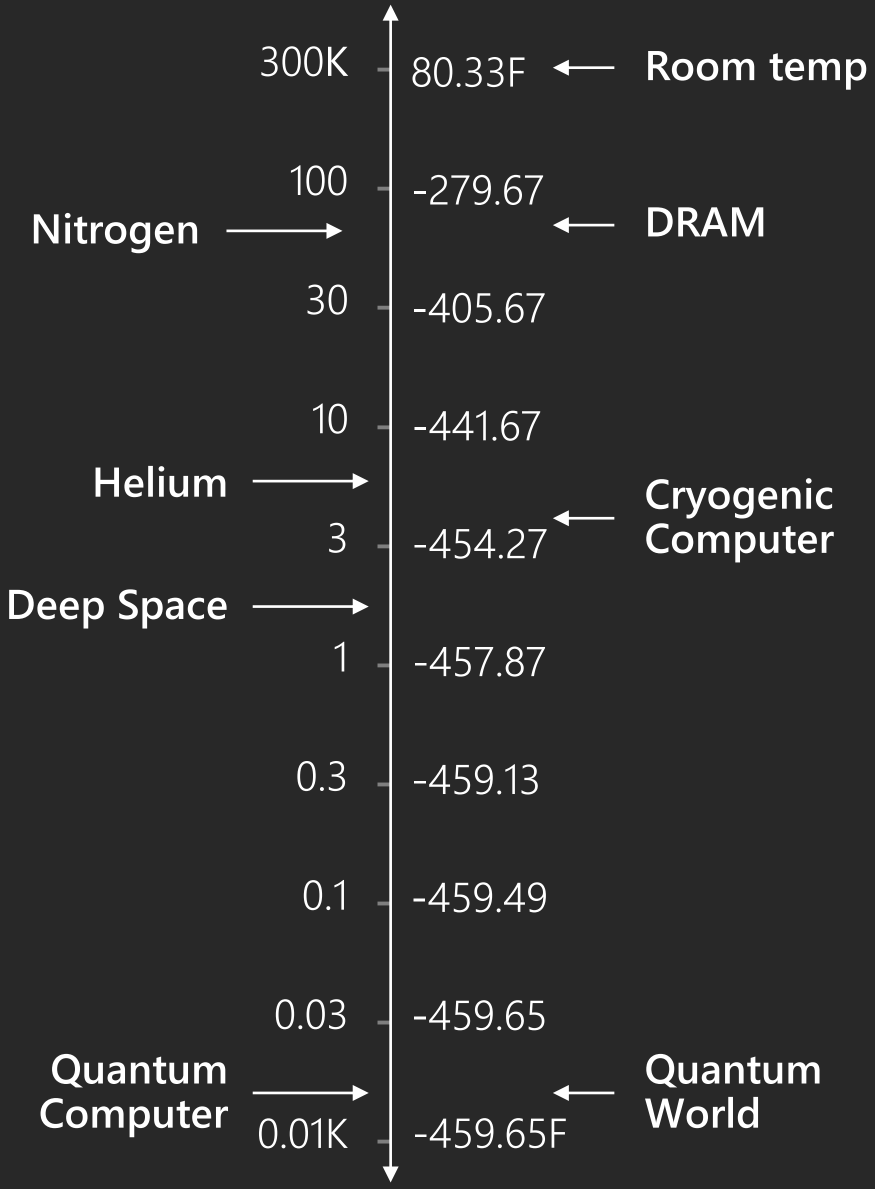
Copenhagen

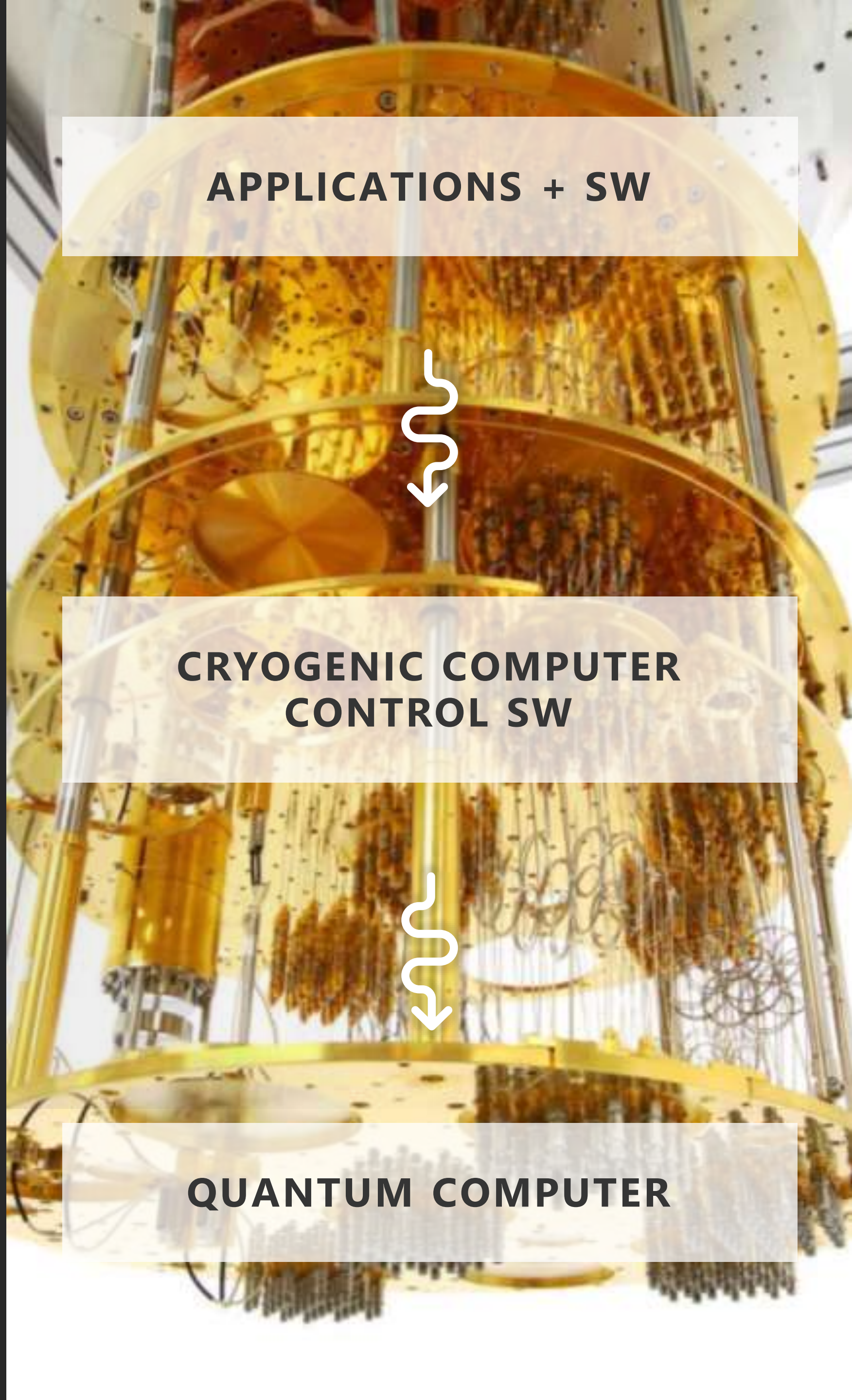
Sydney

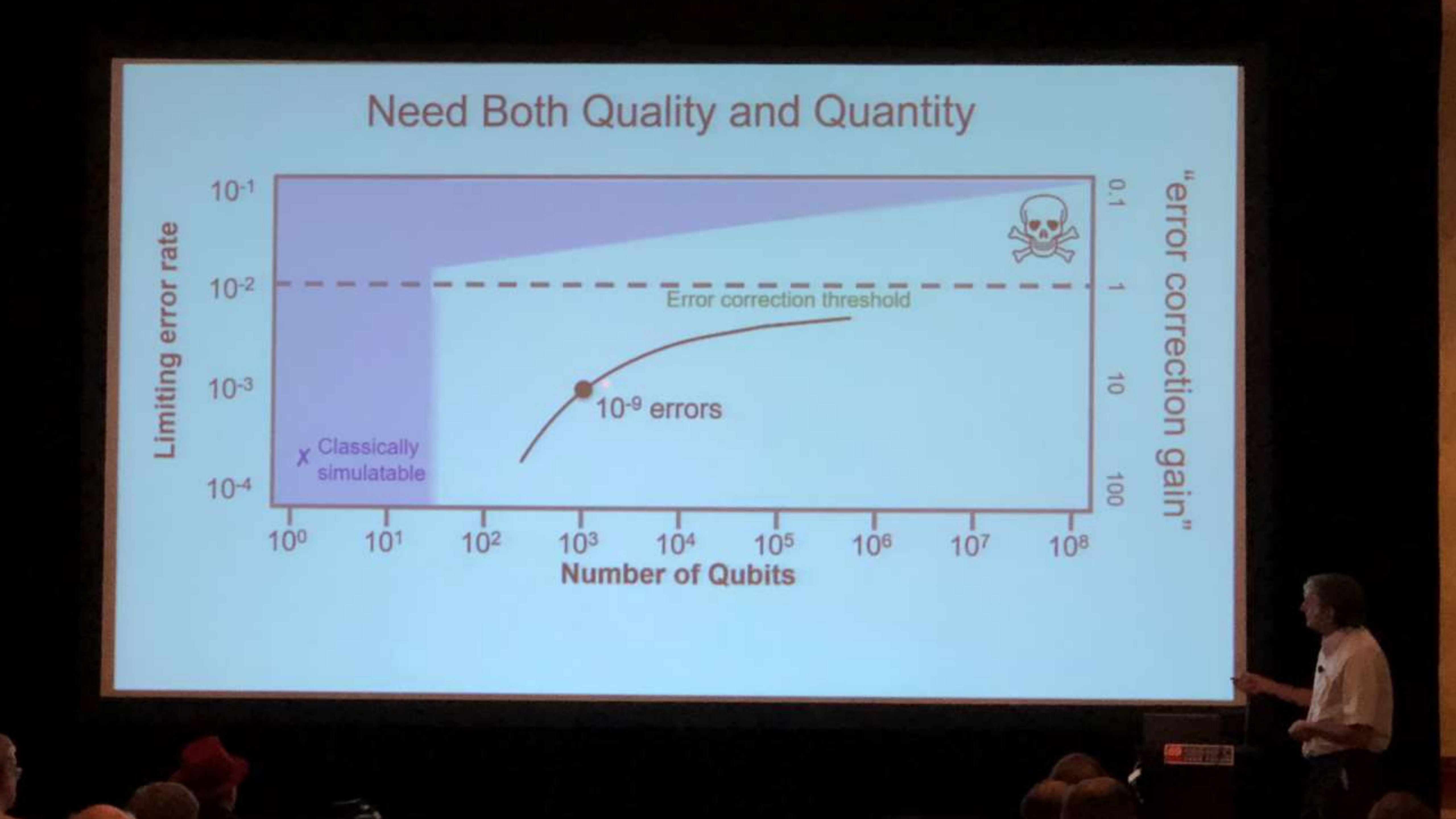
Lafayette

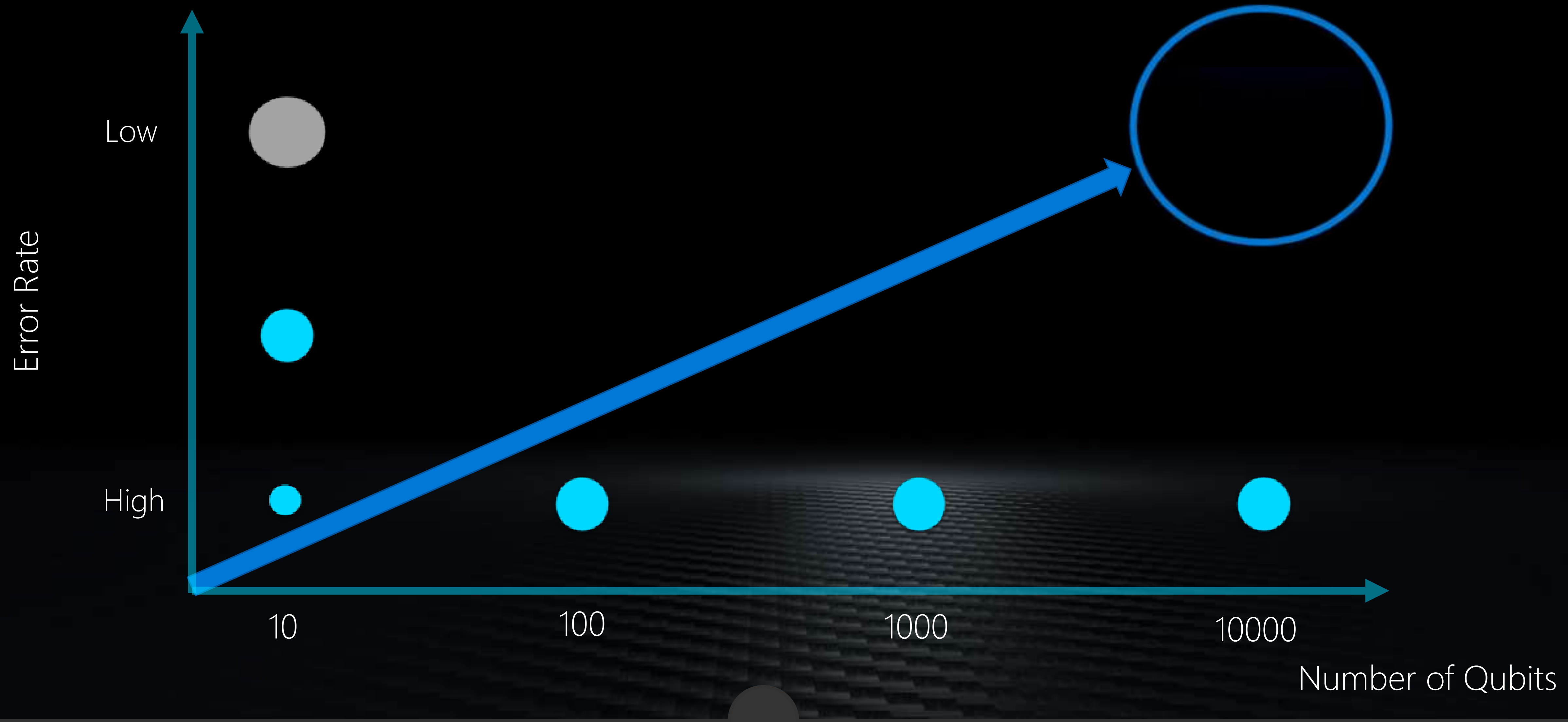





300K
80.33F
Room temp
100
-279.67
Nitrogen
DRAM
30
-405.67
10
-441.67
Helium
Cryogenic Computer
3
-454.27
Deep Space
1
-457.87
0.3
-459.13
0.1
-459.49
0.03
-459.65
Quantum Computer
Quantum World
0.01K
-459.65F


APPLICATIONS + SW
CRYOGENIC COMPUTER CONTROL SW
QUANTUM COMPUTER


Need Both Quality and Quantity
Limiting error rate
10-1
10-2
10-3
10-4
"error correction gain"
0.1
1
10
100
Error correction threshold
10-9 errors
Classically simulatable
10^0
10^1
10^2
10^3
10^4
10^5
10^6
10^7
10^8
Number of Qubits



All qubits are not created equal

Majorana Fermions

Predicted by Ettore Majorana in 1937

"MAJORANA PARTICLE GLIMPSED IN LAB."

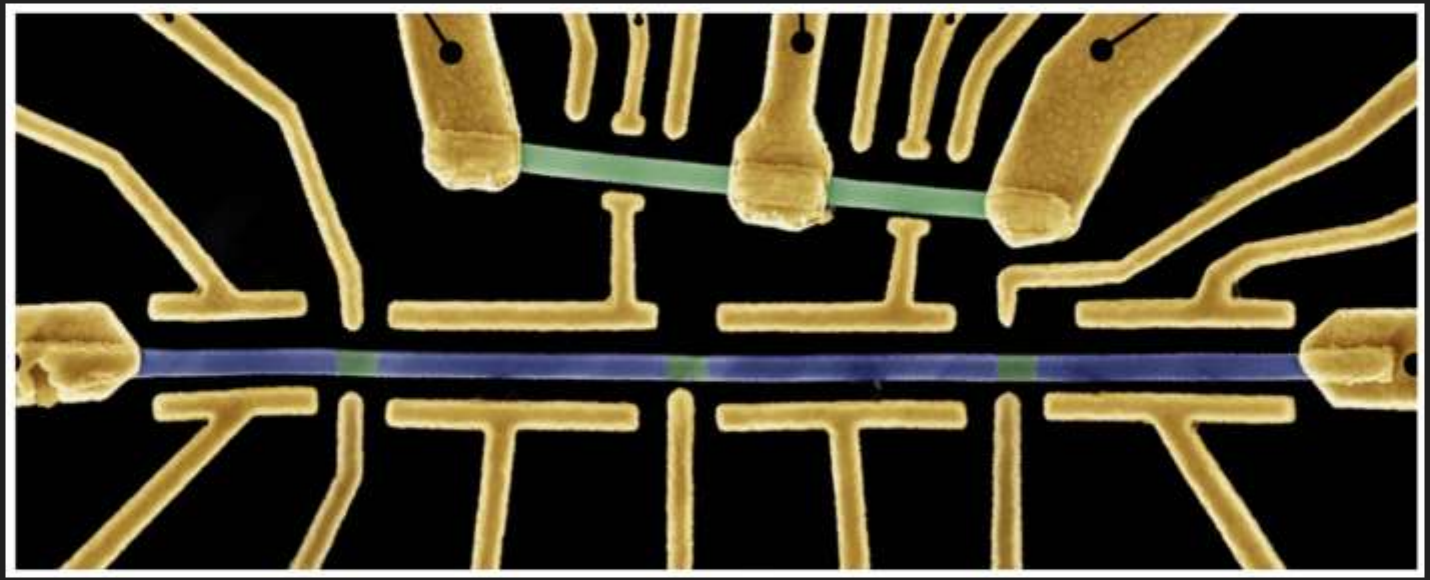
BBC NEWS

2012

Majorana qubits: split the information

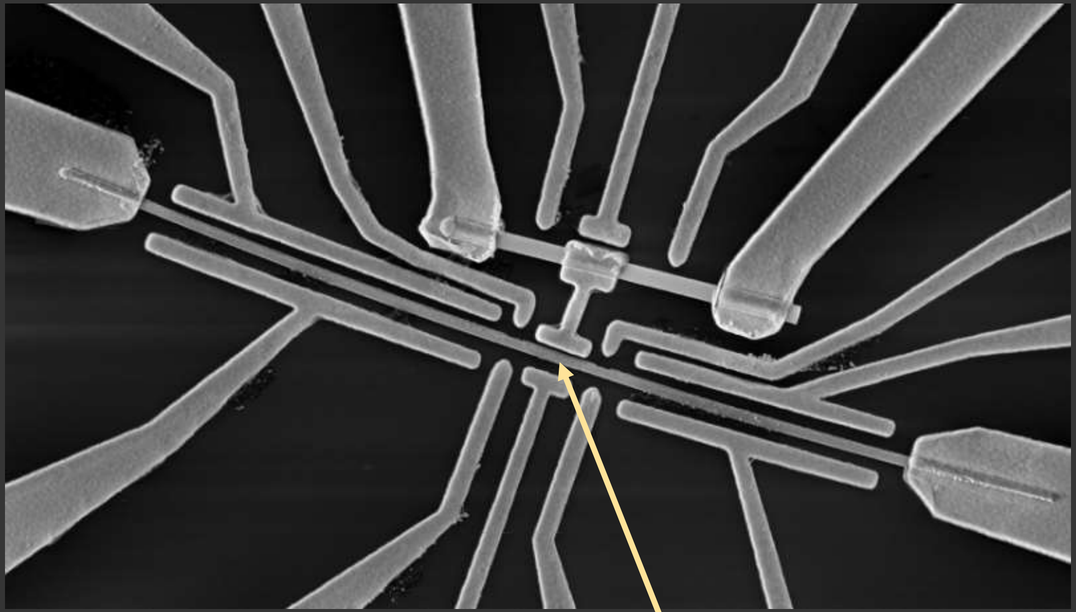
Store a qubit in a superposition of 0 or 1 electrons

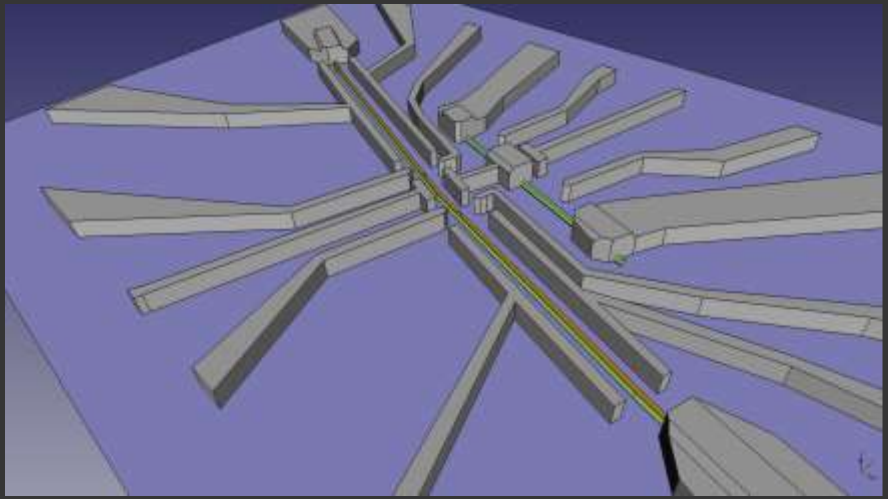
Split 0 or 1 electrons into two “Majorana” particles

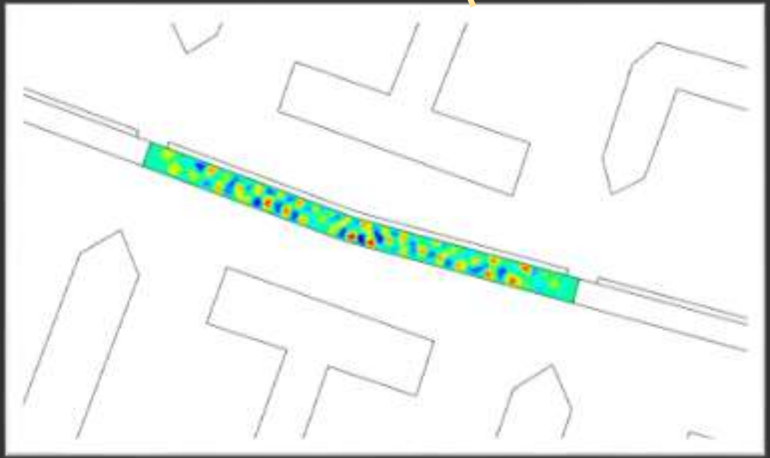


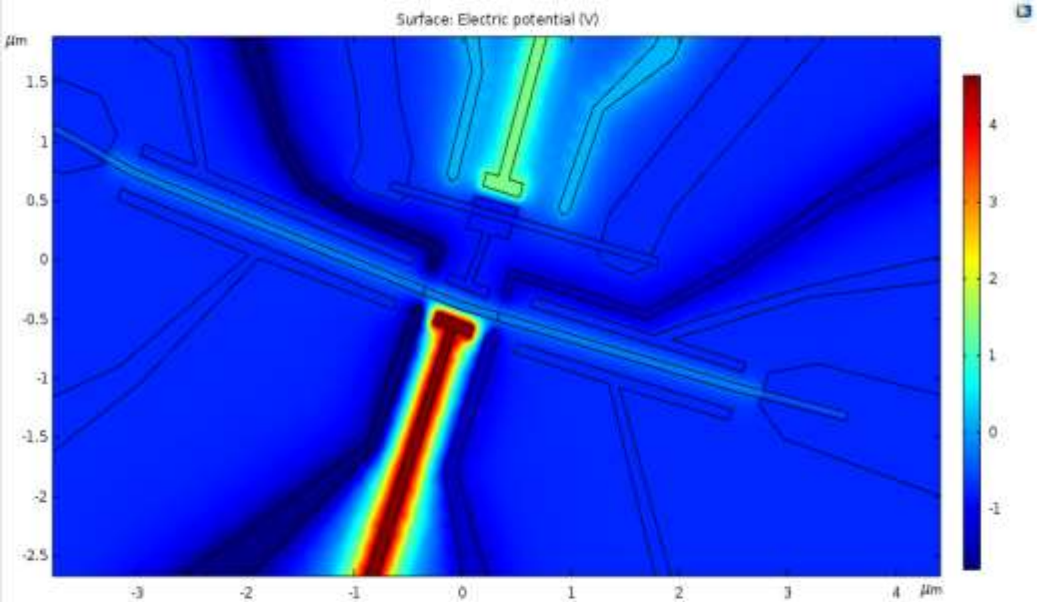
Inca Quipu

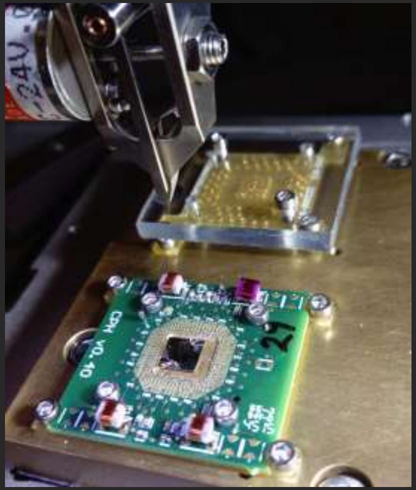
HPC support for qubit design

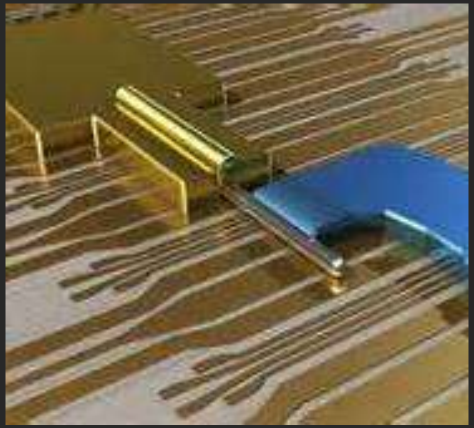




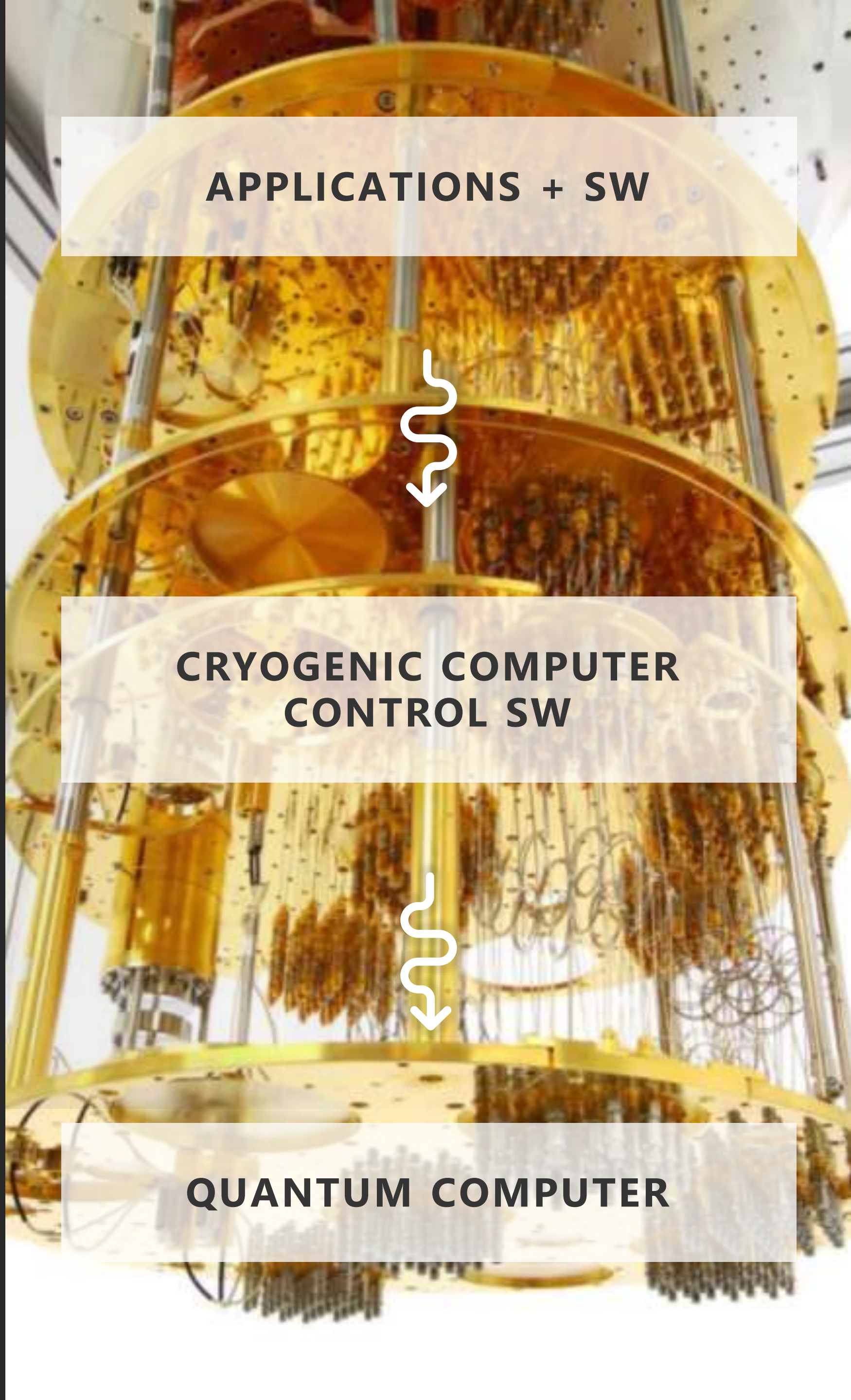






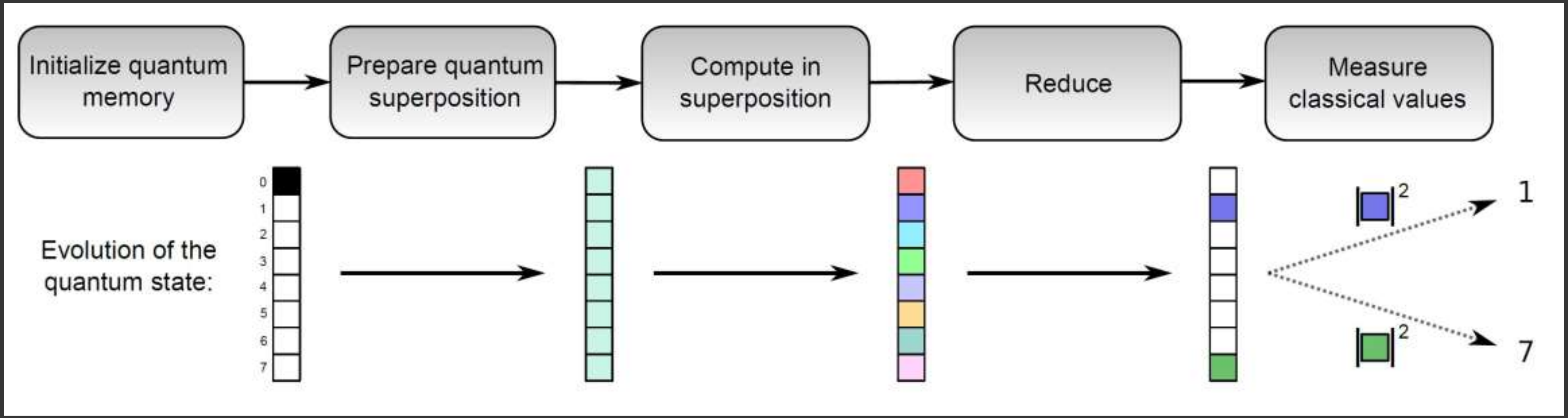


	300K	80.33F	Room temp
	100	-279.67	
Nitrogen			DRAM
	30	-405.67	
	10	-441.67	
Helium			Cryogenic Computer
	3	-454.27	
Deep Space			
	1	-457.87	
	0.3	-459.13	
	0.1	-459.49	
	0.03	-459.65	
Quantum Computer			Quantum World
	0.01K	-459.65F	



Computing in superposition

~~Quantum computers are fast because they operate on all values simultaneously~~



It’s not that easy!

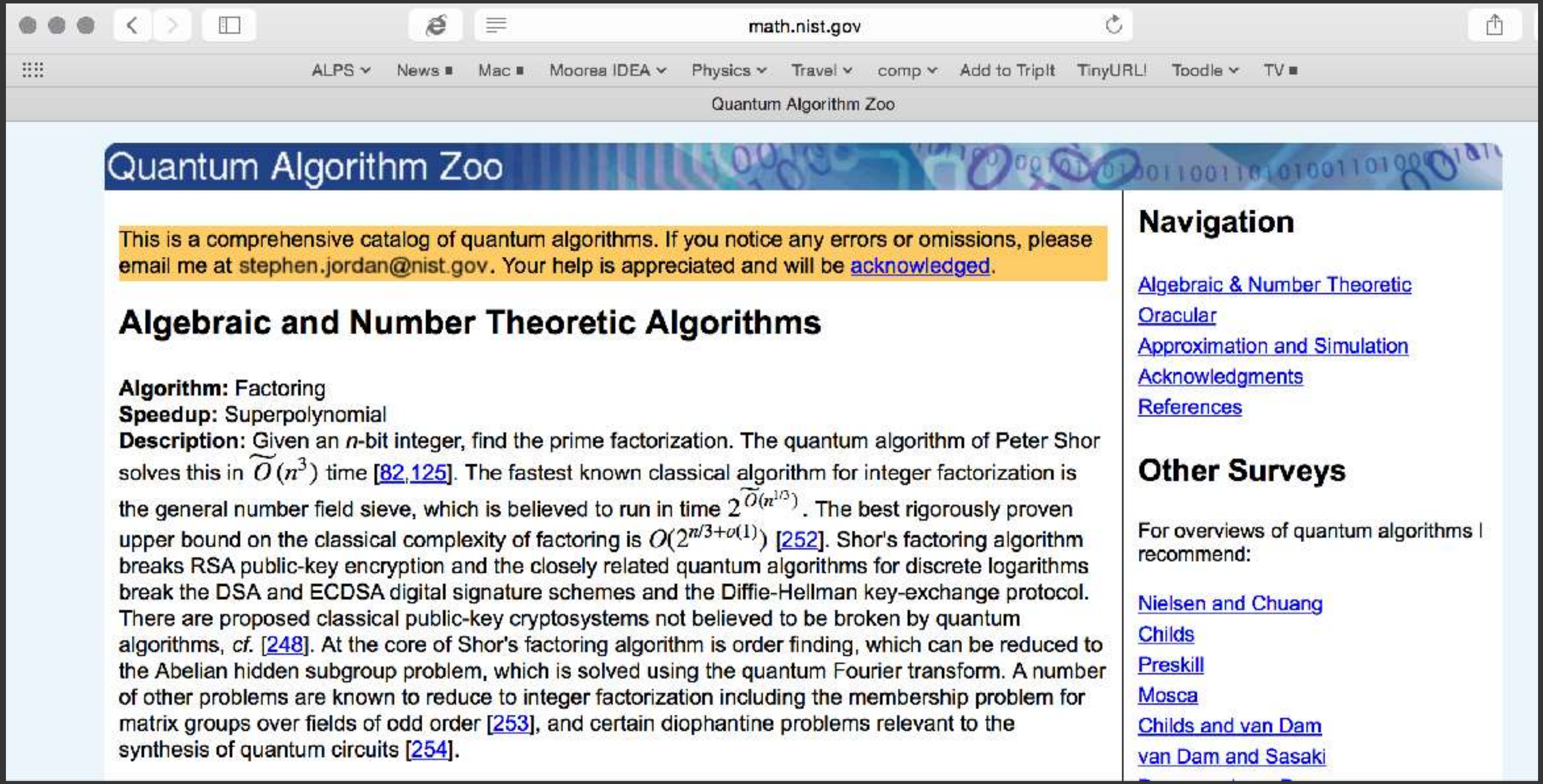
- Reading out the superposition only gives us a single random entry
- The crucial aspect of quantum algorithm design is finding good reduction operations that lead to (almost) deterministic asnwers

Developing quantum applications

1. Find quantum algorithm with quantum speedup

Quantum algorithms with quantum speedup

50+ quantum algorithms with quantum speedup, that is better asymptotic scaling than any classical computer



math.nist.gov

ALPS News Mac Mooras IDEA Physics Travel comp Add to TripIt TinyURL! Toodle TV

Quantum Algorithm Zoo

Quantum Algorithm Zoo

This is a comprehensive catalog of quantum algorithms. If you notice any errors or omissions, please email me at stephen.jordan@nist.gov. Your help is appreciated and will be acknowledged.

Algebraic and Number Theoretic Algorithms

Algorithm: Factoring
Speedup: Superpolynomial
Description: Given an *n*-bit integer, find the prime factorization. The quantum algorithm of Peter Shor solves this in $\widetilde{O}(n^3)$ time [82,125]. The fastest known classical algorithm for integer factorization is the general number field sieve, which is believed to run in time $2^{\widetilde{O}(n^{1/3})}$. The best rigorously proven upper bound on the classical complexity of factoring is $O(2^{n/3+o(1)})$ [252]. Shor's factoring algorithm breaks RSA public-key encryption and the closely related quantum algorithms for discrete logarithms break the DSA and ECDSA digital signature schemes and the Diffie-Hellman key-exchange protocol. There are proposed classical public-key cryptosystems not believed to be broken by quantum algorithms, *cf.* [248]. At the core of Shor's factoring algorithm is order finding, which can be reduced to the Abelian hidden subgroup problem, which is solved using the quantum Fourier transform. A number of other problems are known to reduce to integer factorization including the membership problem for matrix groups over fields of odd order [253], and certain diophantine problems relevant to the synthesis of quantum circuits [254].

Navigation

Algebraic & Number Theoretic
Oracular
Approximation and Simulation
Acknowledgments
References

Other Surveys

For overviews of quantum algorithms I recommend:

Nielsen and Chuang
Childs
Preskill
Mosca
Childs and van Dam
van Dam and Sasaki

http://math.nist.gov/quantum/zoo/

Developing quantum applications

quantum software engineers

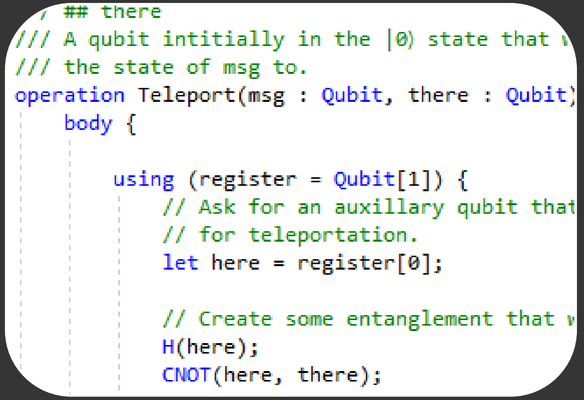
1. Find quantum algorithm with quantum speedup

2. Confirm quantum speedup after implementing all subroutines and I/O

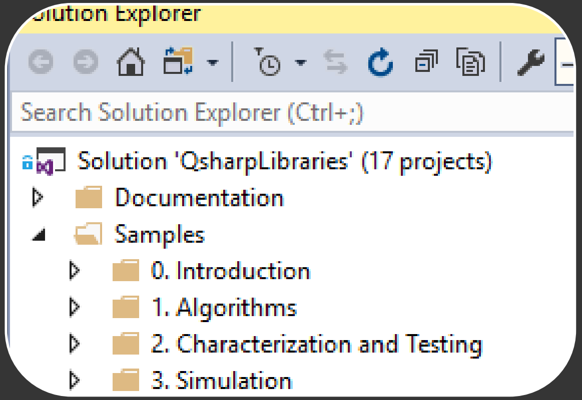
3. Optimize code until runtime is short enough

4. Embed into specific architecture and estimate resources

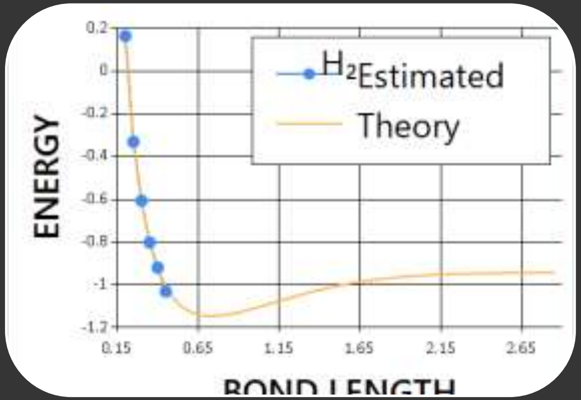
Introducing the
Microsoft Quantum Development Kit



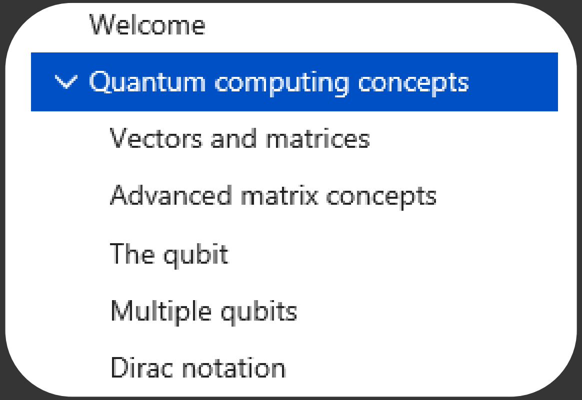
Quantum programming language Q#



Visual Studio integration and debugging



Local and cloud quantum simulation



Extensive open-source libraries, samples, documentation

Target machines

- State-of-the-Art Local Simulator
  - Simulate 30 qubits in 16 GB
  - Run locally on your PC
- State-of-the-Art Azure Simulator
  - Simulate more than 40 qubits
  - Run in Azure
- Trace Simulator
  - Determine resource costs of quantum program
  - Scale to large algorithms and numbers of qubits
- Quantum Computer

Distributed simulator using MPI

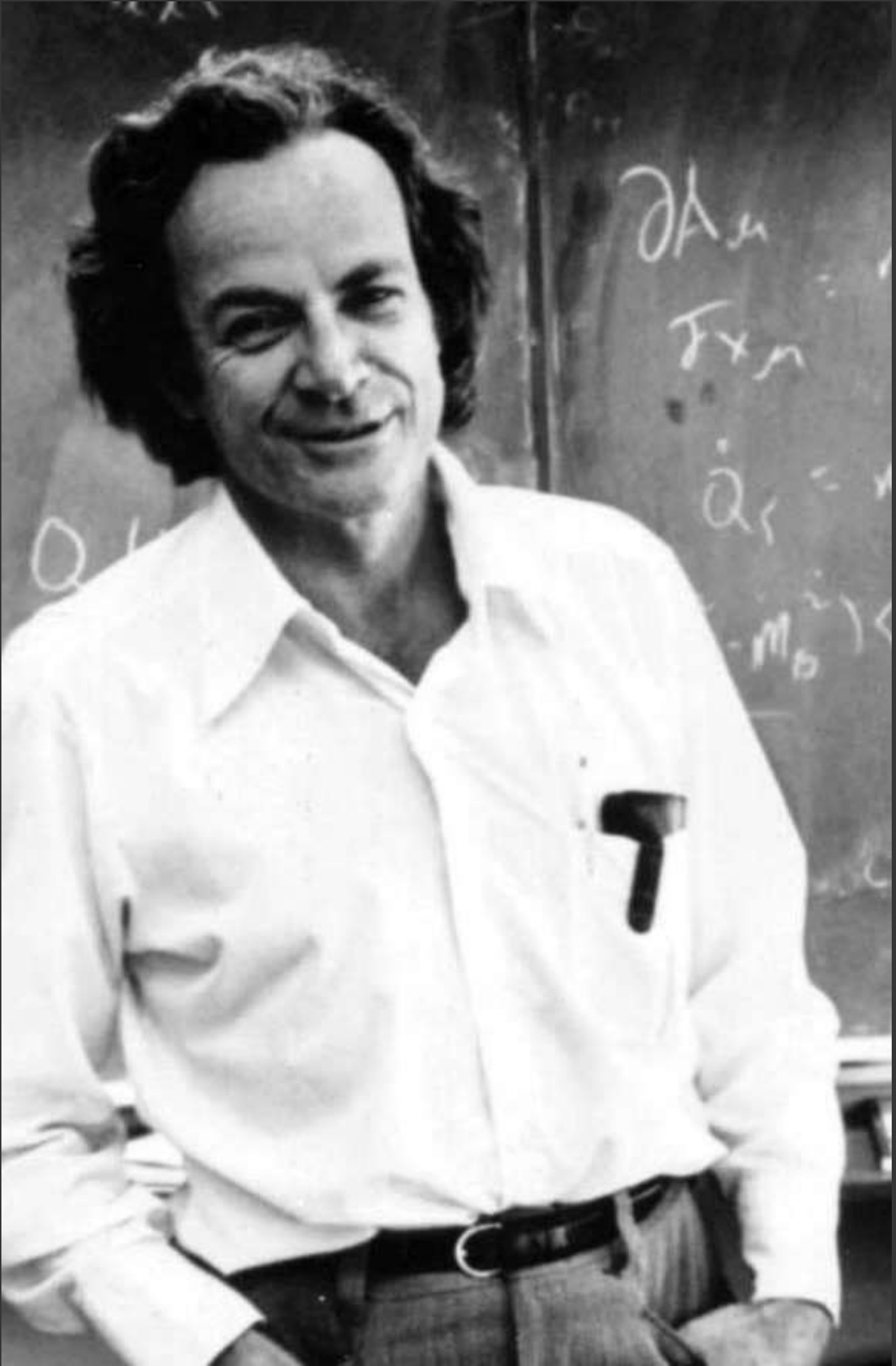
2017: supercomputer

2018: cloud

MPI-based distributed simulator, similar to that of ETH students D. Steiger and T. Häner

More than 30x reduction in network traffic compared to other simulators (SC'17 paper)

No need to buy a supercomputer: available as Azure HPC cloud services up to ≈43 qubits



International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

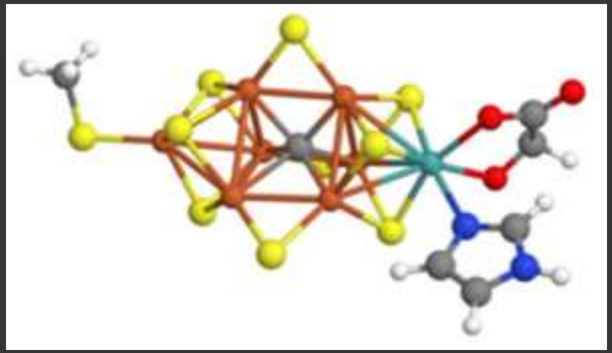
Received May 7, 1981

Feynman proposed to use quantum computers to simulate quantum physics

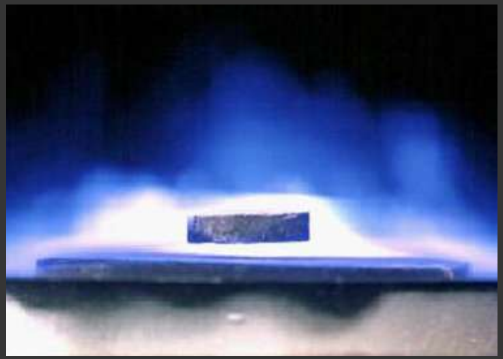
We can surpass the best classical computers with only 50 qubits!

There are many classical algorithms for simulating quantum systems, but they all have limited applicability.

Chemistry



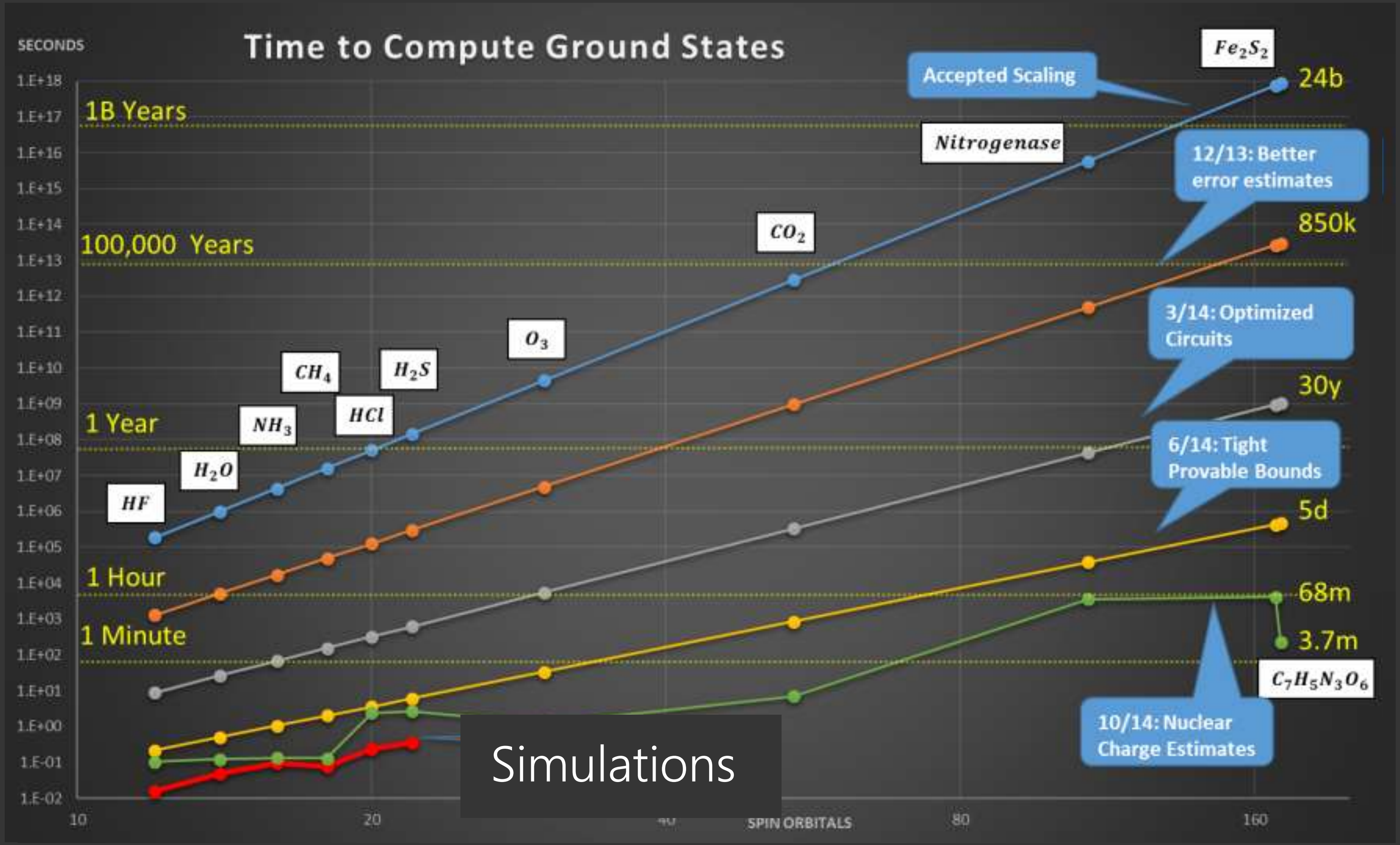
Materials



Nuclear and Particle Physics

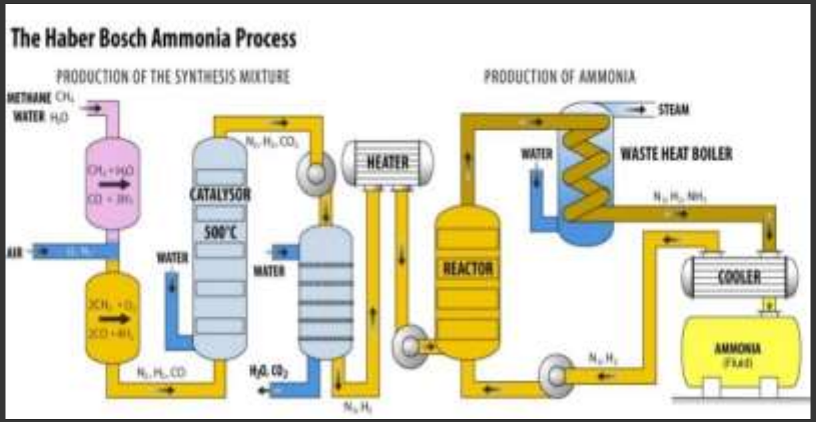
Many problems are out of reach even for exascale supercomputers but doable on quantum computers.

Simulation Evidence

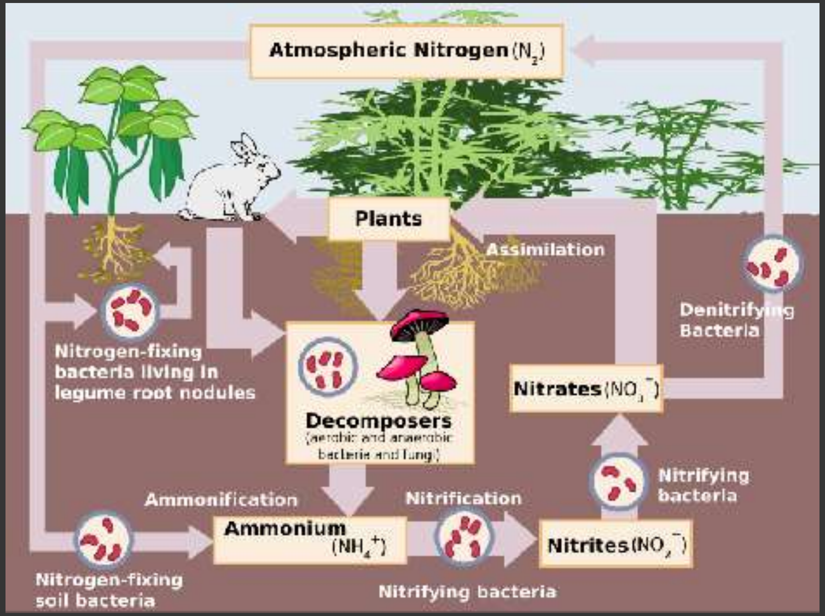


Nitrogen fixation

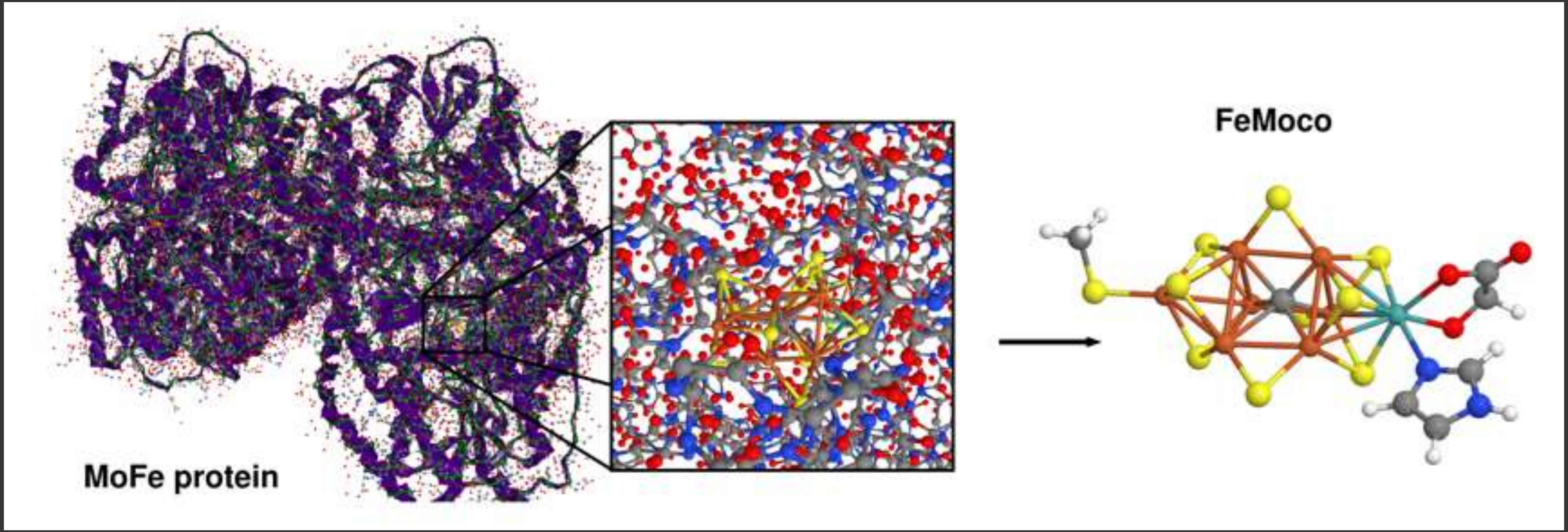
Fertilizer production using Haber-Bosch process needs 3% of the world's natural gas production



But bacteria can do it in the soil without a huge factory!



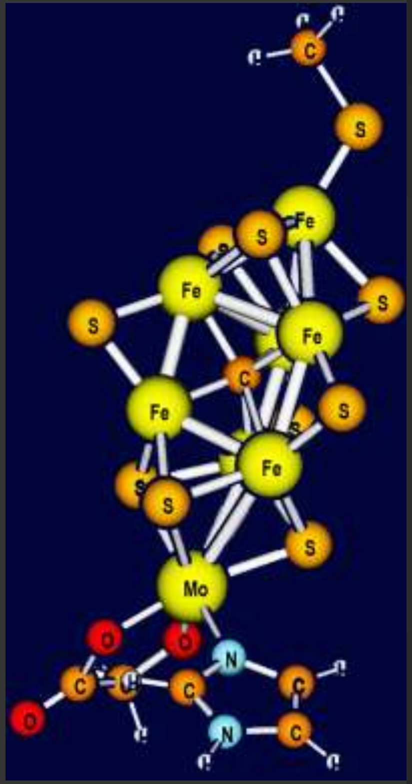
Understanding biological nitrogen fixation

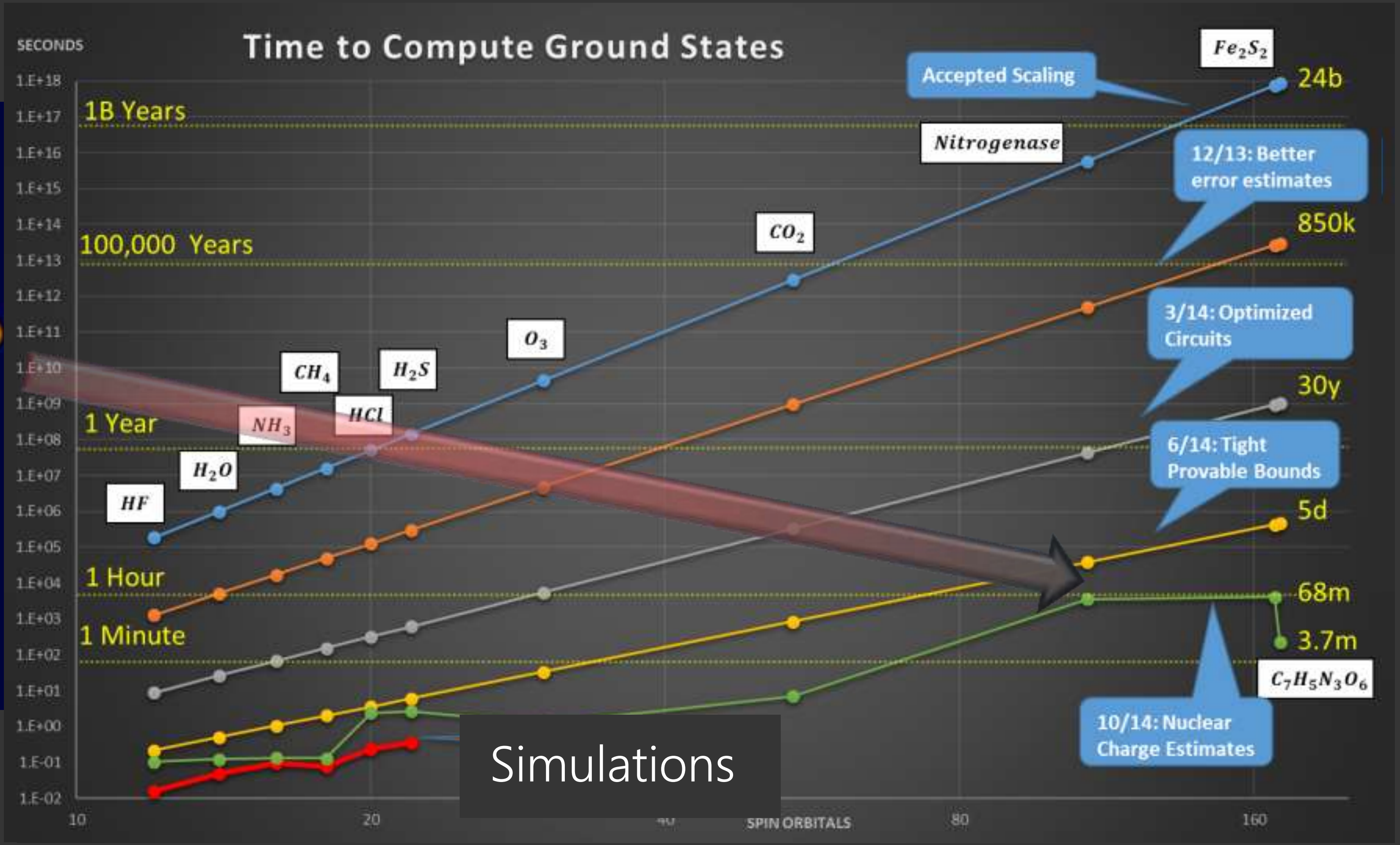


Intractable on classical supercomputers

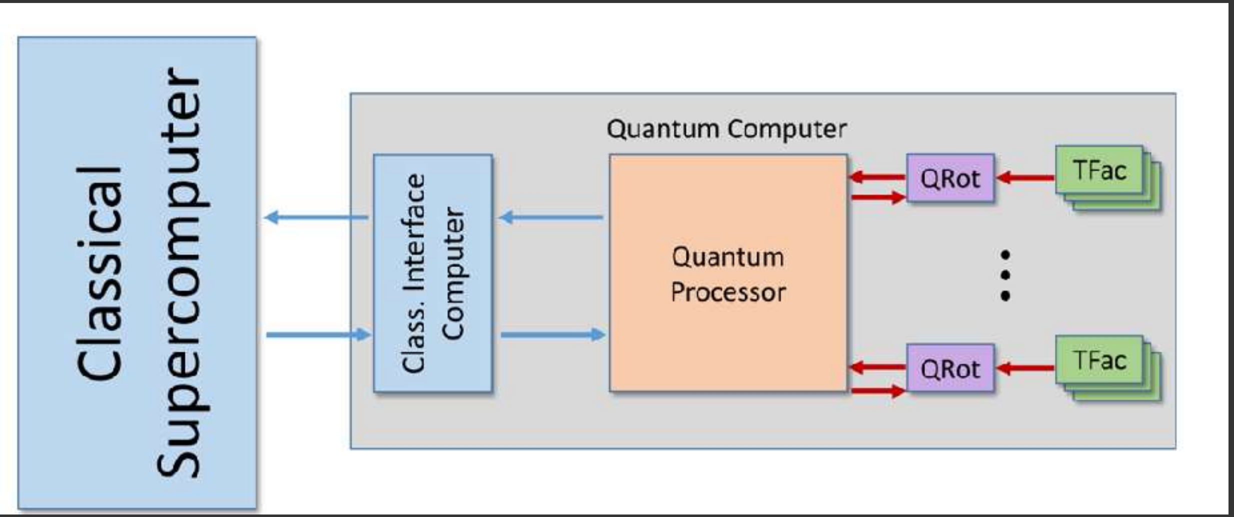
But a 200-qubit quantum computer will let us understand it

Simulation Evidence





Total cost with quantum error correction



	Nested rotations		
Error Rate	10^{-3}	10^{-6}	10^{-9}
Required code distance	37,17	9	5
	Quantum processor		
Logical qubits	109		

10^8 10^6 10^5

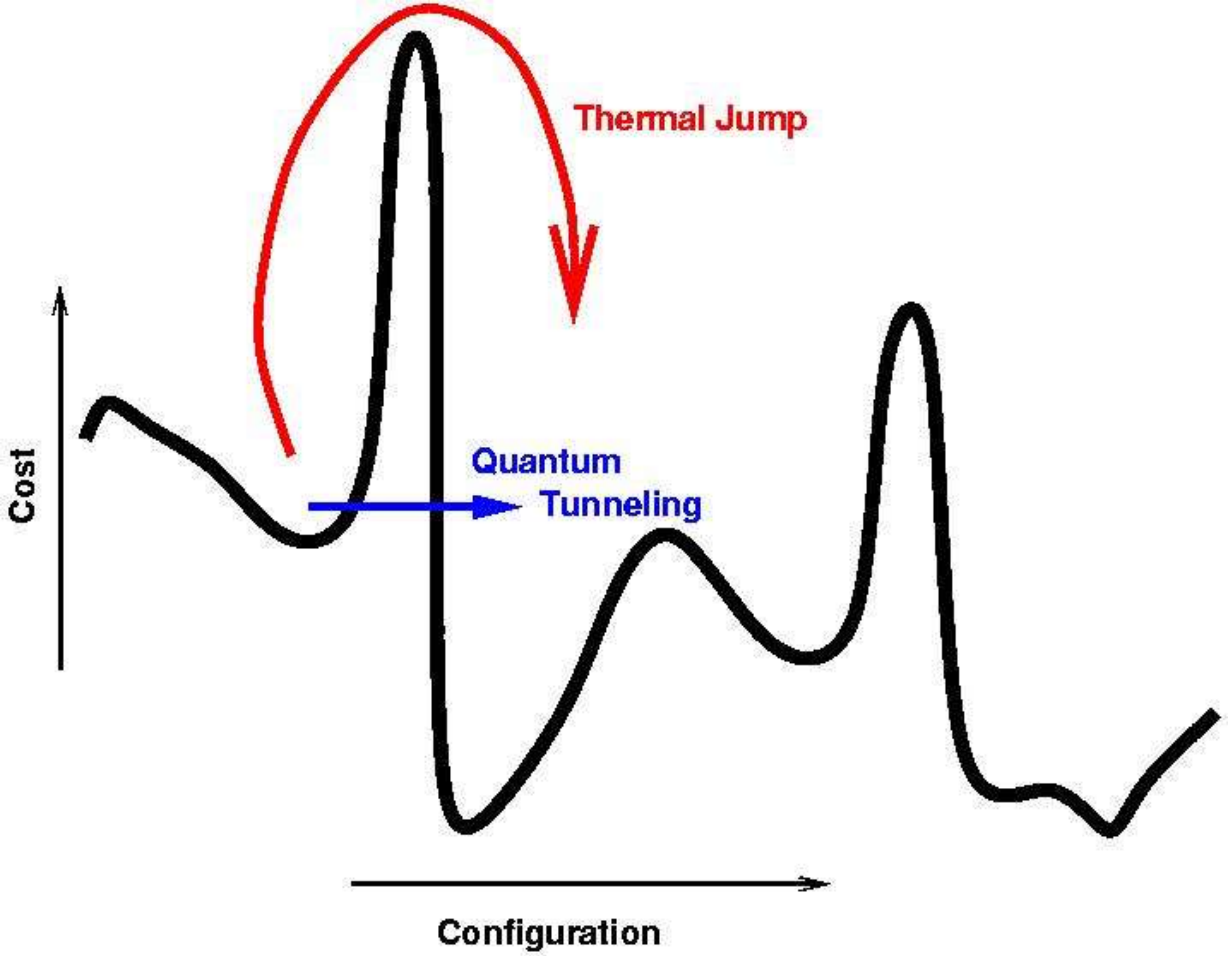
We need better qubits!

Better algorithms!

Better quantum error correction (Hastings & Haah)

Quantum optimization

Use quantum effects to escape local minima
by tunneling under a barrier

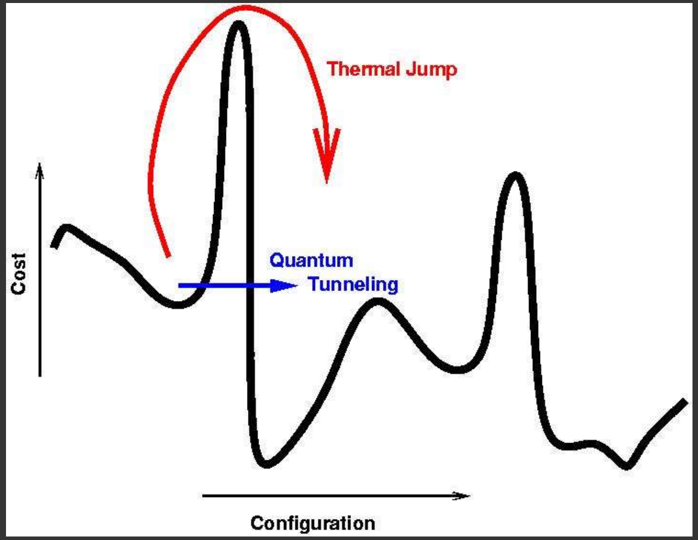


Early value: quantum inspired optimization

Mimic quantum tunneling
on classical computers today!

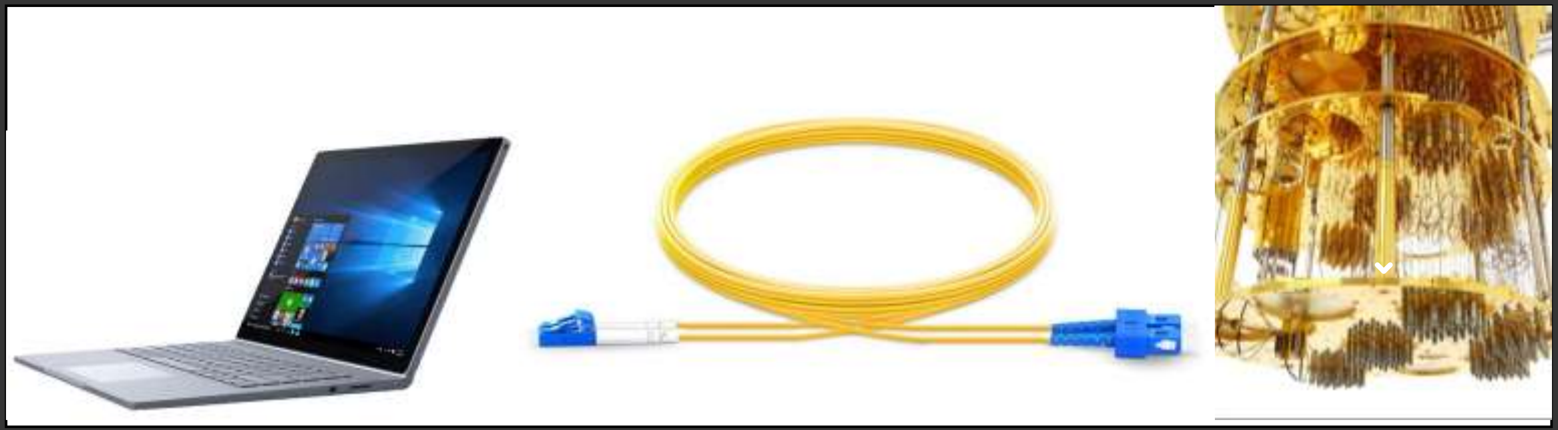
Research into quantum algorithms often
uncovers new classical algorithms

Better optimization methods
Better training algorithms
Better models for machine learning



Will cloud service respect privacy of my data?
Will the computation be implemented correctly?

Blind quantum computation can certify privacy and correctness of delegated computation.
(Broadbent, Fitzsimons, Kashefi, 2009)



It is time to start writing quantum software

Invent new quantum algorithms
Explore quantum applications
Determine resources and optimize quantum code
Co-design quantum hardware and software