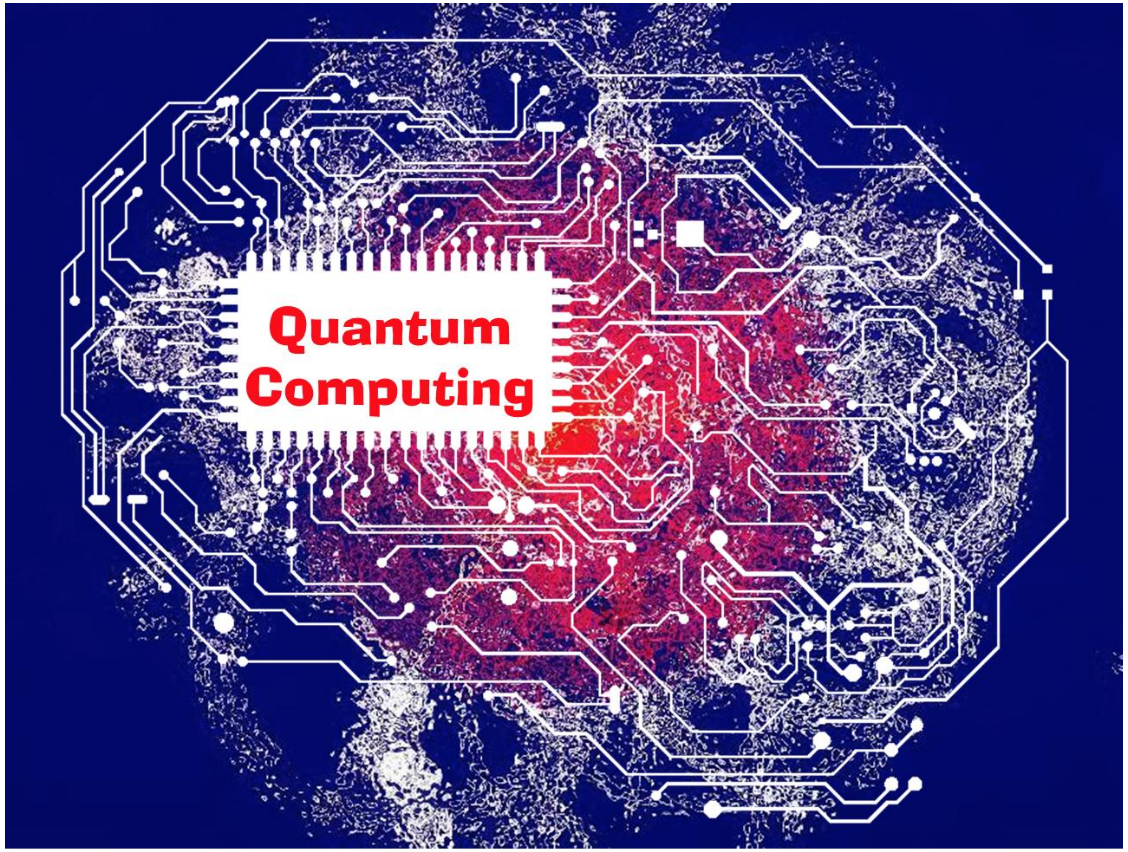
Quantum Computing: Technology, Market and Ecosystem Overview



Raffaele Mauro
Managing Director
Endeavor Italy

DGI Report Presentation
Milano
January, 2020

Finance & Venture Capital

Policy Innovation

Technology

Why Quantum Computing ? Why now ?

Scientific relevance

Potential extension of the Moore's Law for specific domains

Spike in funding and commercial activity

Media Hype ....

Google moves toward quantum supremacy with 72-qubit computer

IBM and Intel recently debuted similarly sized chips

BY EMILY CONOVER 5:17PM, MARCH 5, 2018

IBM Quantum Computer Does Record-Breaking Chemistry

Ryan F. Mandelbaum

Oct 16, 2017, 9:00am · Filed to: ibm

Share

NSA Says It "Must Act Now" Against the Quantum Computing Threat

The National Security Agency is worried that quantum computers will neutralize our best encryption – but doesn't yet know what to do about that problem.

Y Combinator's quantum computing 'spaceshot' scores $64M from A16Z, others

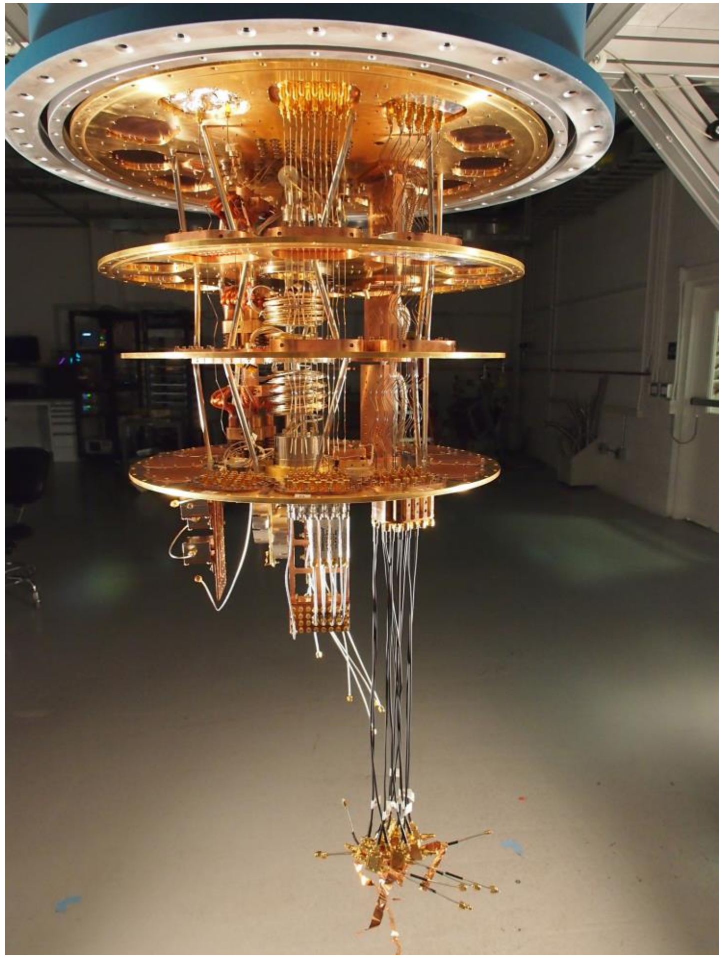
China is opening a new quantum research supercenter

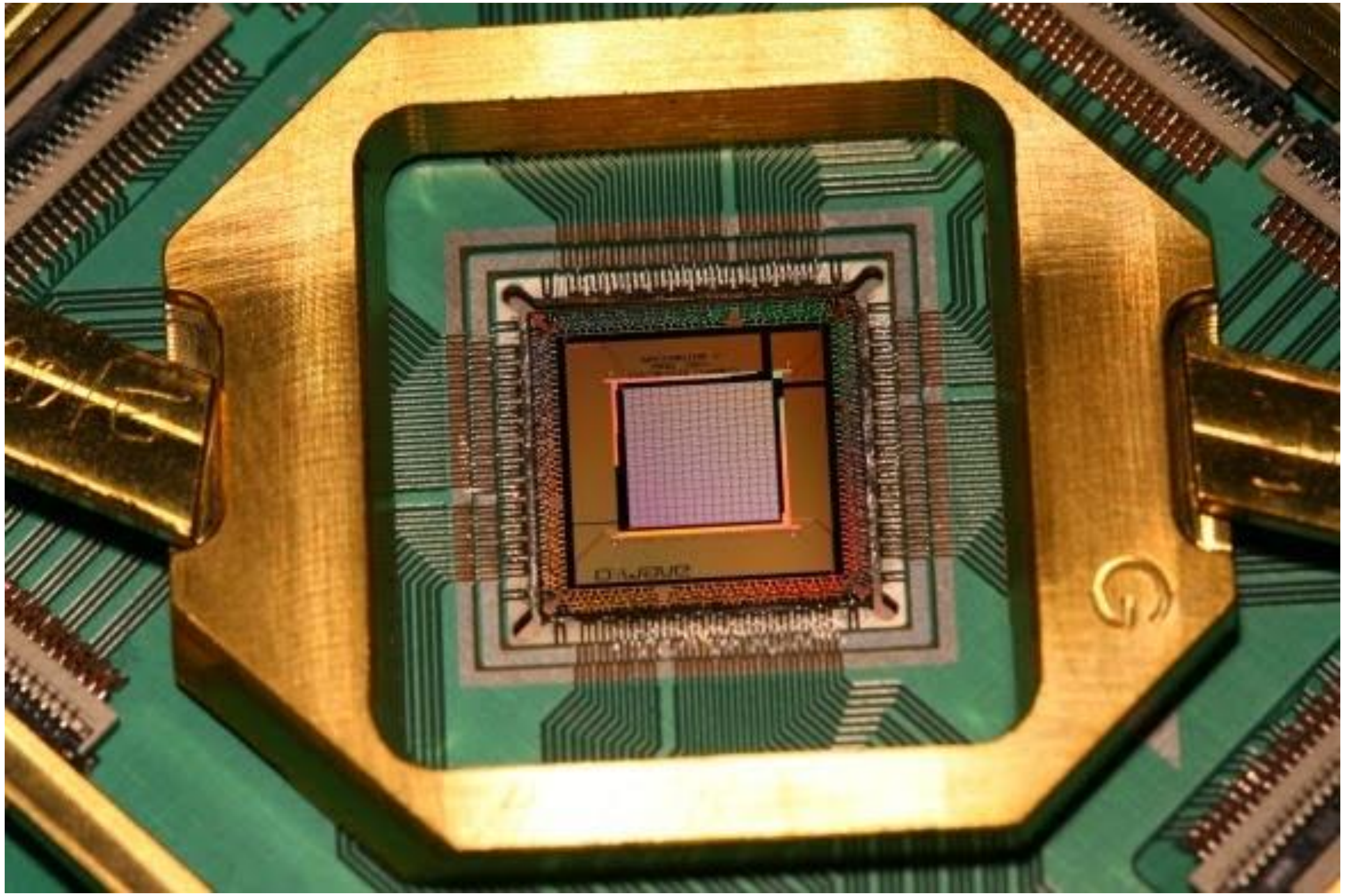
The country wants to build a quantum computer with a million times the computing power of all others presently in the world.

Alibaba is spending $15 billion on researching quantum computing, AI, and more

The e-commerce giant looks overseas for R&D to move beyond its roots

… but very, very hard engineering problems yet to be solved

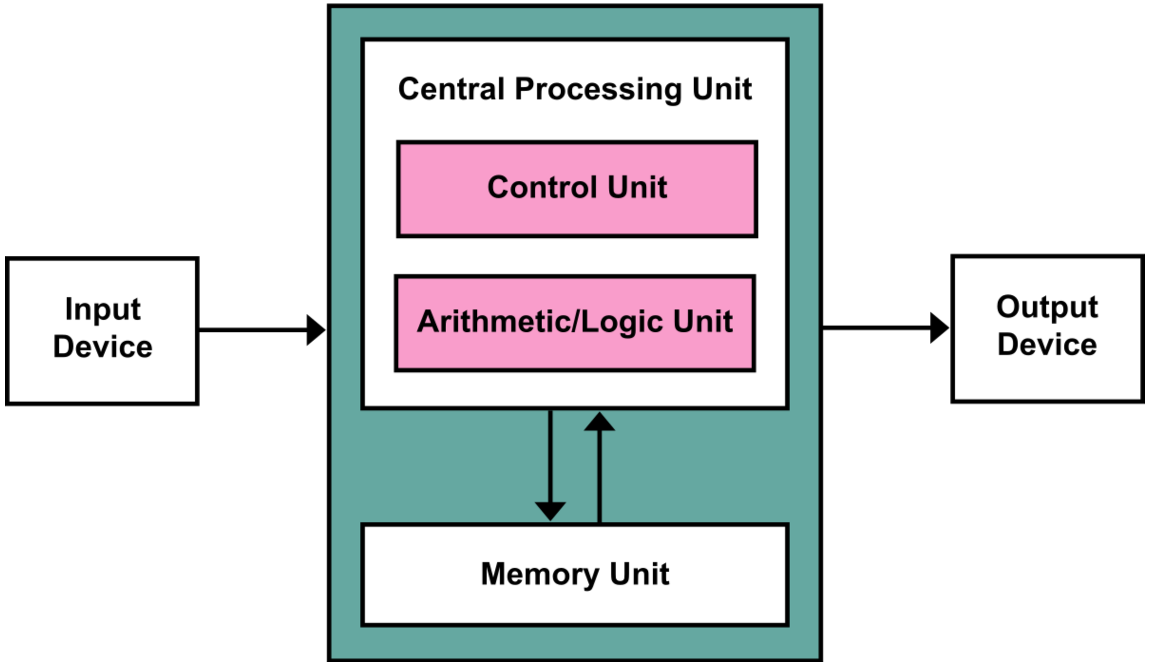




Computation as we know it

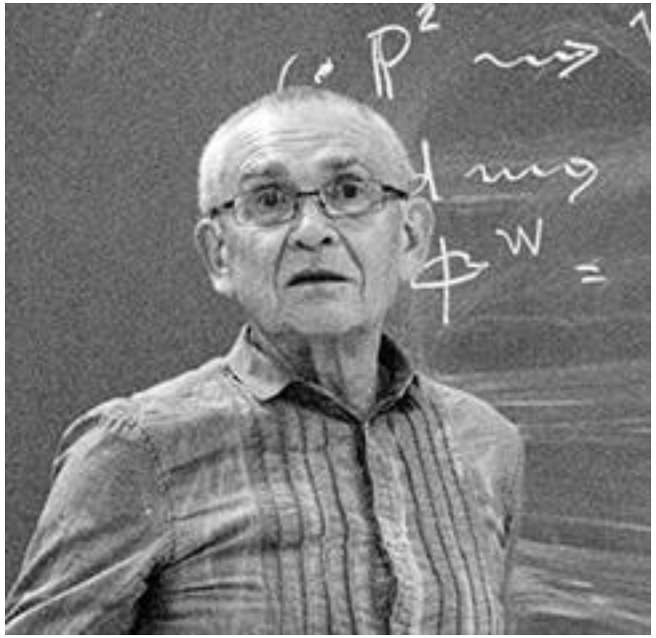
Information codified in bits

Processed by Von Neumann Machines

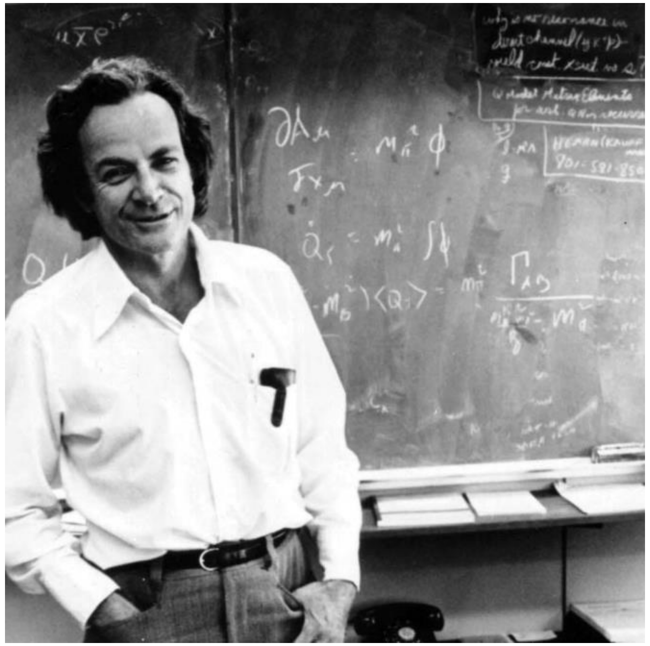


80’s: The Beginning

Yuri Manin



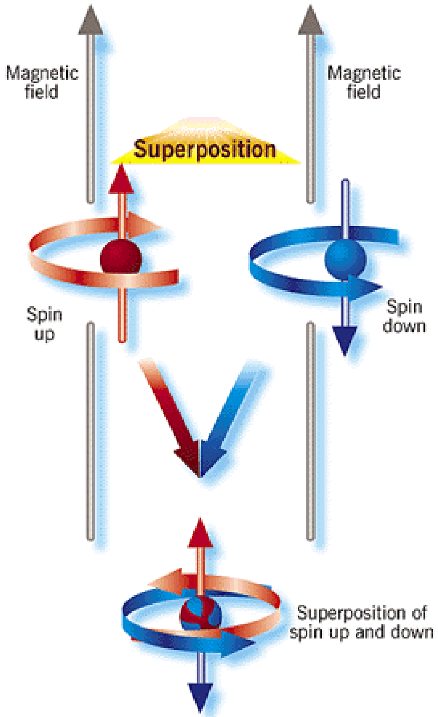
Richard Feynamn



David Deutsch

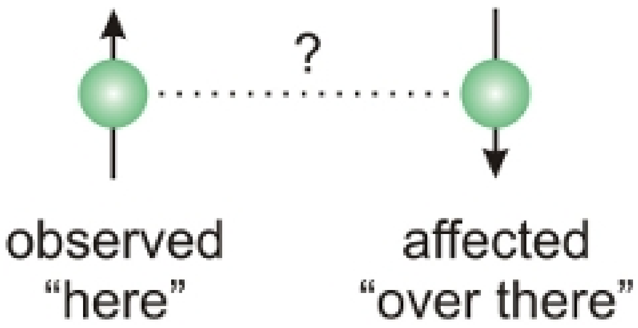
Quantum Properties

Superposition



Simultaneus "existence" (pre-measurement) of different states

Entanglement



Correlation of two different systems

Qubits

Qubit:
|Q>=a|1>+b|0>

a) Superposition of states 1 and 0
=> Qubits encode **more information** than a traditional bit

b) Entangled qubits could encode an exponentially large numebr of states.

c) Interference allows higher probability of obtaining desired solutions

=> **Speed up** in calculation

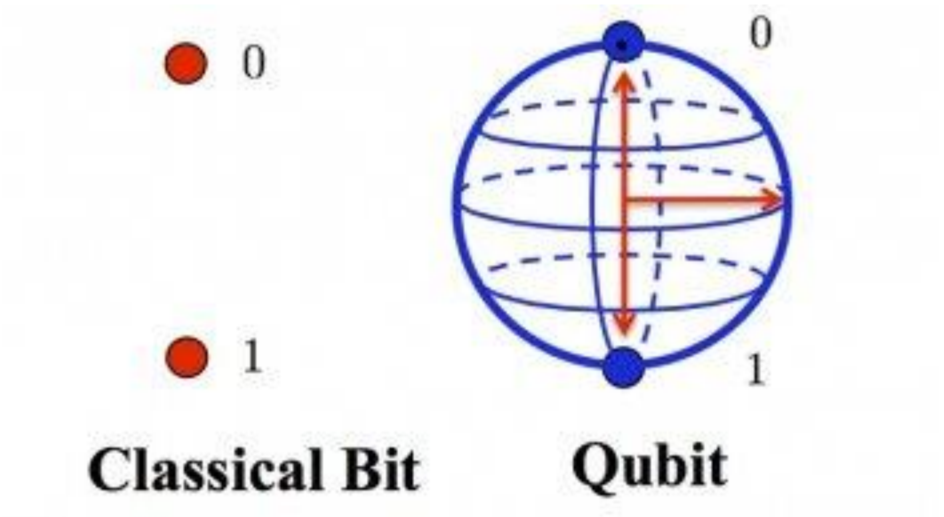
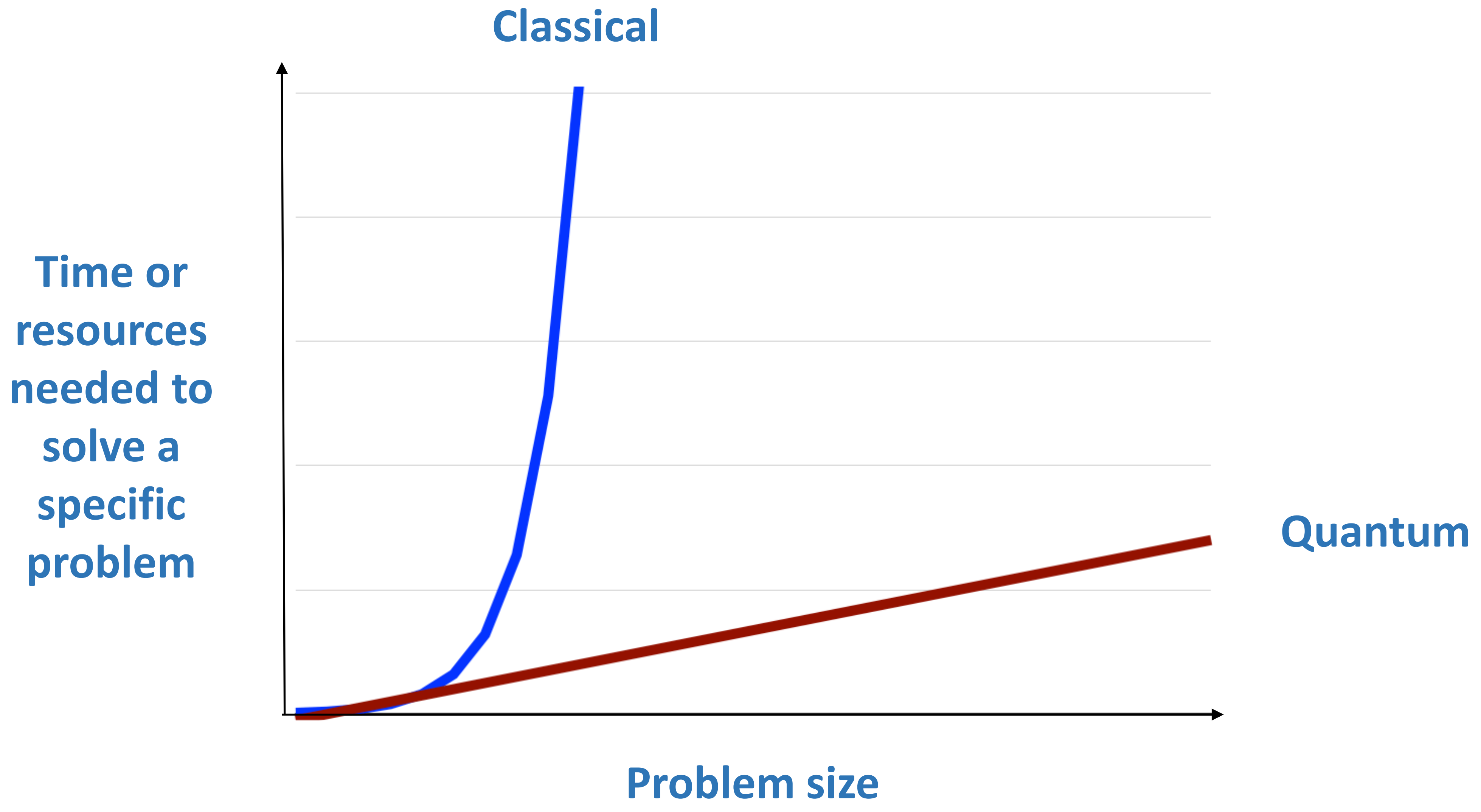


Image source: Wikimedia

Computation Time: Classical Vs Quantum



Dispelling misconceptions

"Basically, people think they'll be magic oracles that will solve all problems faster, rather than just ***special classes*** *of problems"*

Scott Aaronson

Solving complex problems … Only some of them !

Example:
Prime factorization

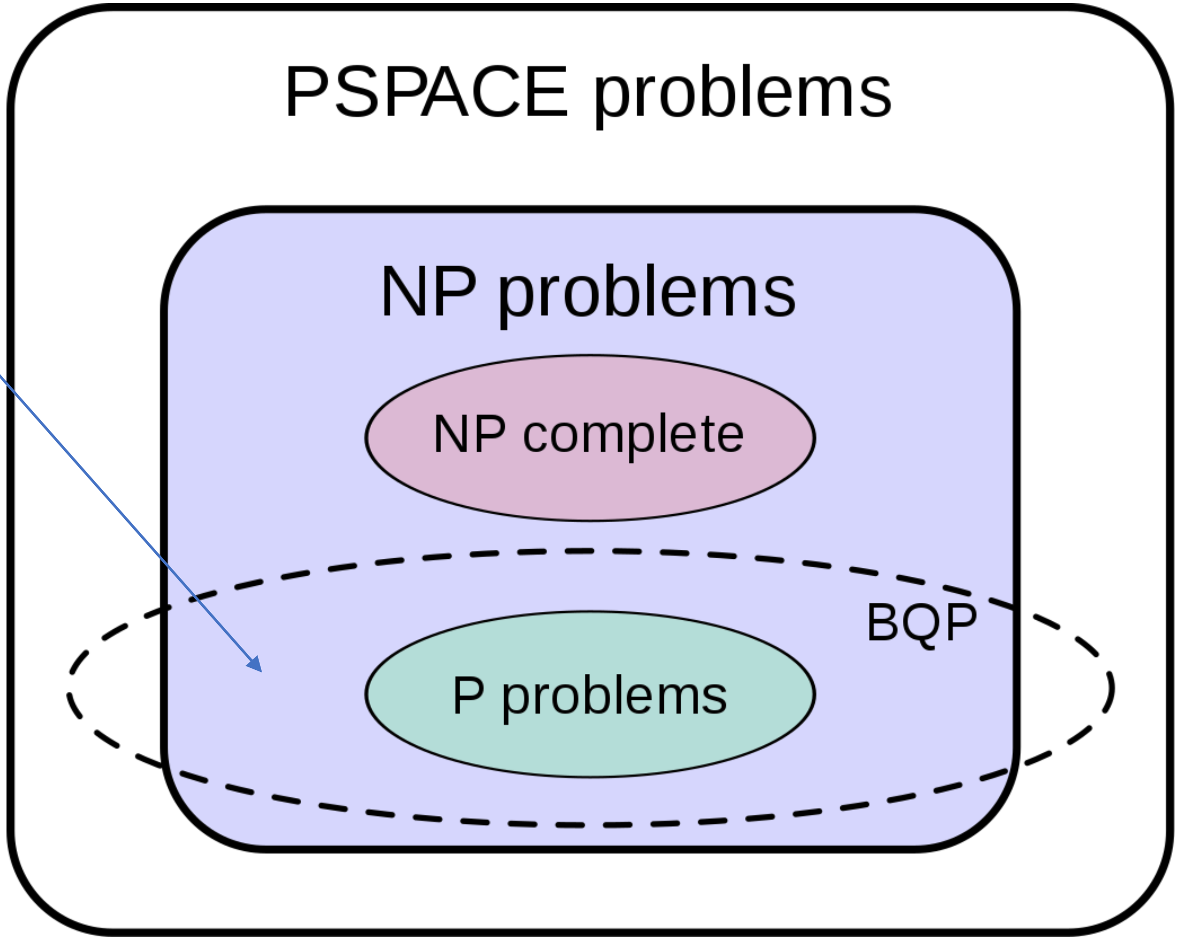


Image source: Wikimedia

90’s: Quantum Computing and Theoretical Computer Science

1994: Factorization problems

- Shor algorithm
- Potential application in cryptography
- Exponential speedup (in comparison with classical computing)

1996: Search problems

- Grover algorithm
- Applications in software engineering / databases
- Quadratic speedup

00's & 10's: Technical Infrastructure

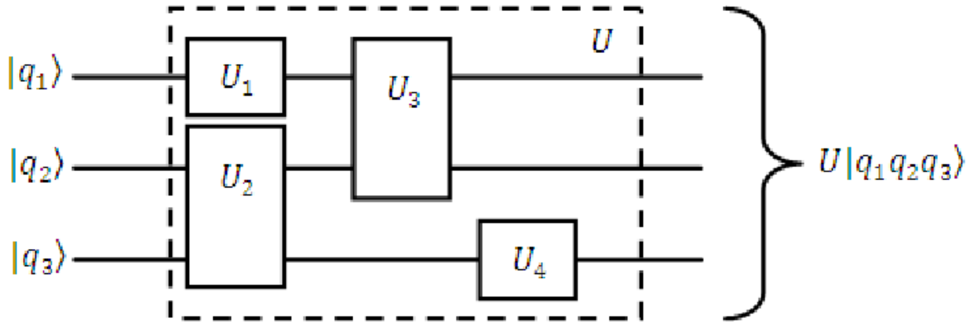
Different approaches:

- Solid state spin qubits
- Ion-based qubits
- Superconducting qubits
- Optical qubits
- Topological qubits
- Etc. …

Image source: IBM

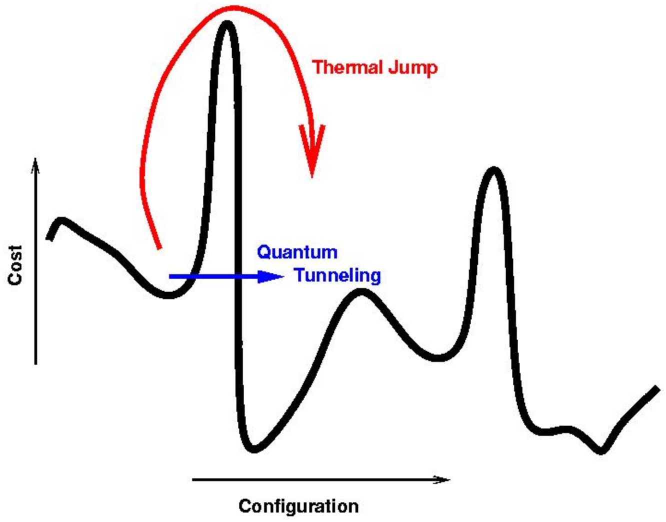
Two Major Technological Paradigms

Circuit Model



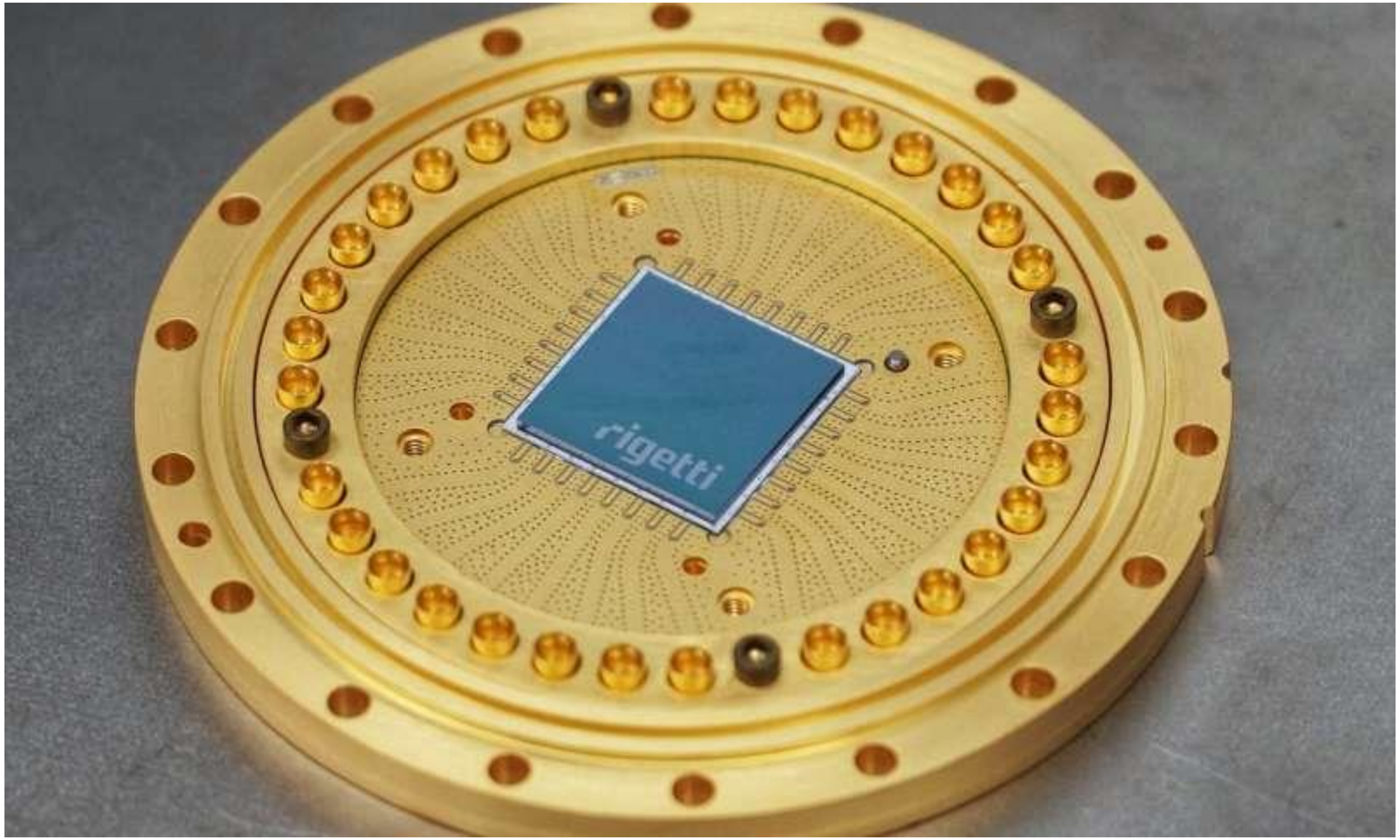
- Logical Gates
- Predictable behaviour at scale
- ”Mainstream” approach
- IBM, Google, Righetti

Adiabatic Model



- Math problem solved phisically
- Solutions are low energy states
- Hard to predict behaviour at scale
- No error correction
- D-Wave, Google

10's: Quantum chips with < 100 Qubits



2019: Quantum Supremacy!

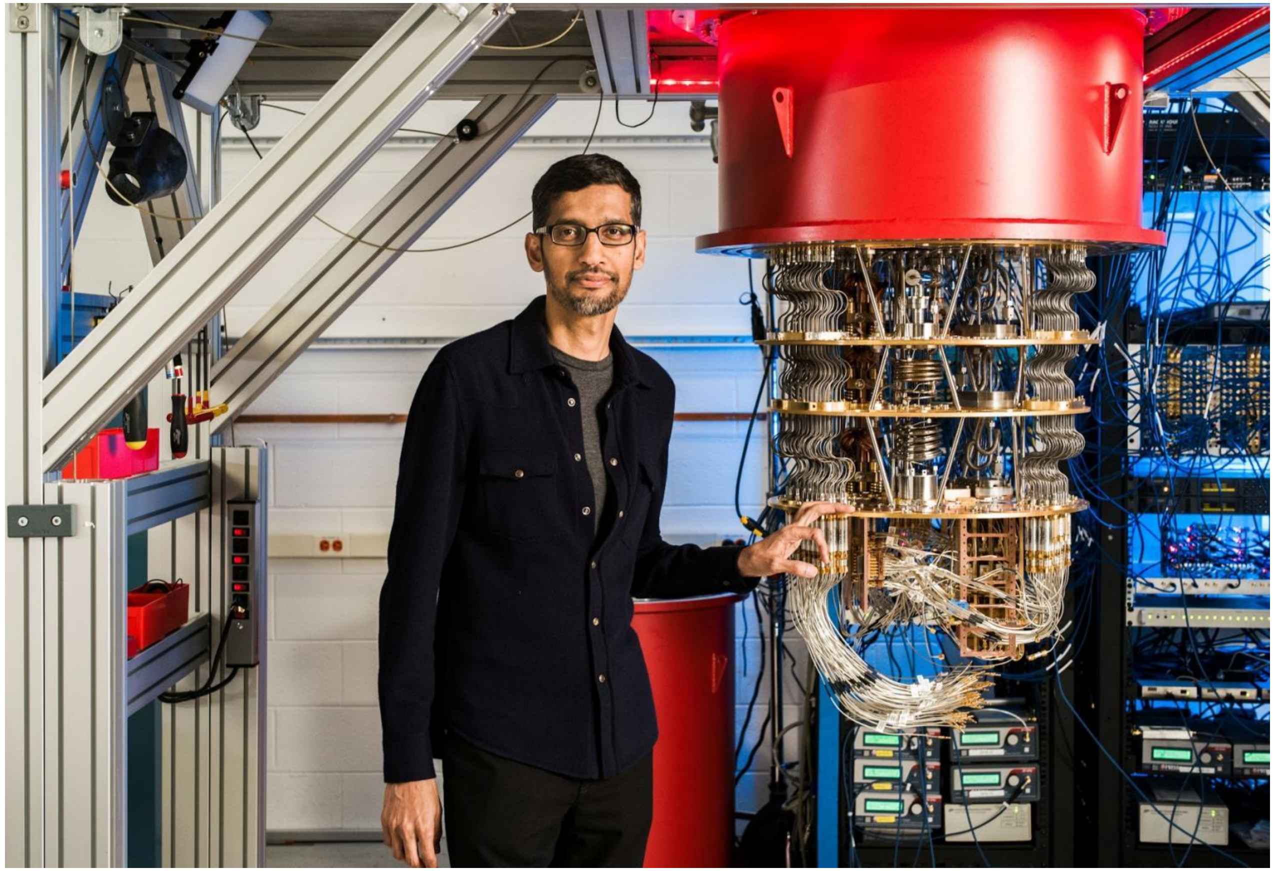


Image source: Reuters – In the photo: Sundar Pichai, CEO at Google

Empirical demonstration of quantum speedup

Bringing attention and funds

2020s: Solving issues in Q.C.

Hardware:

- Decoherence / instability / noise
- Almost absolute zero-degree temperature for some architectures

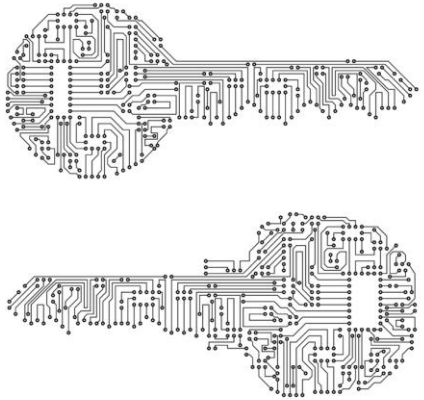
Software:

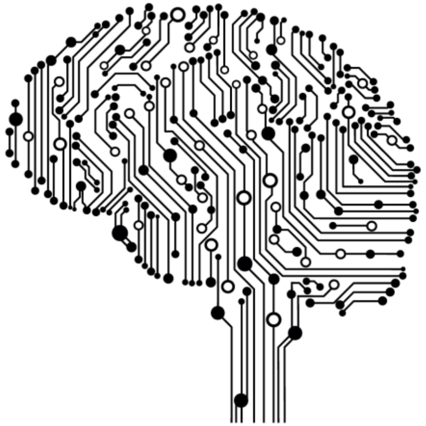
- Error correction -> Adding more qubits not useful with high error rate
- Millions of qubits needed for some applications

Timing:

- Real commercial applications probably far in time

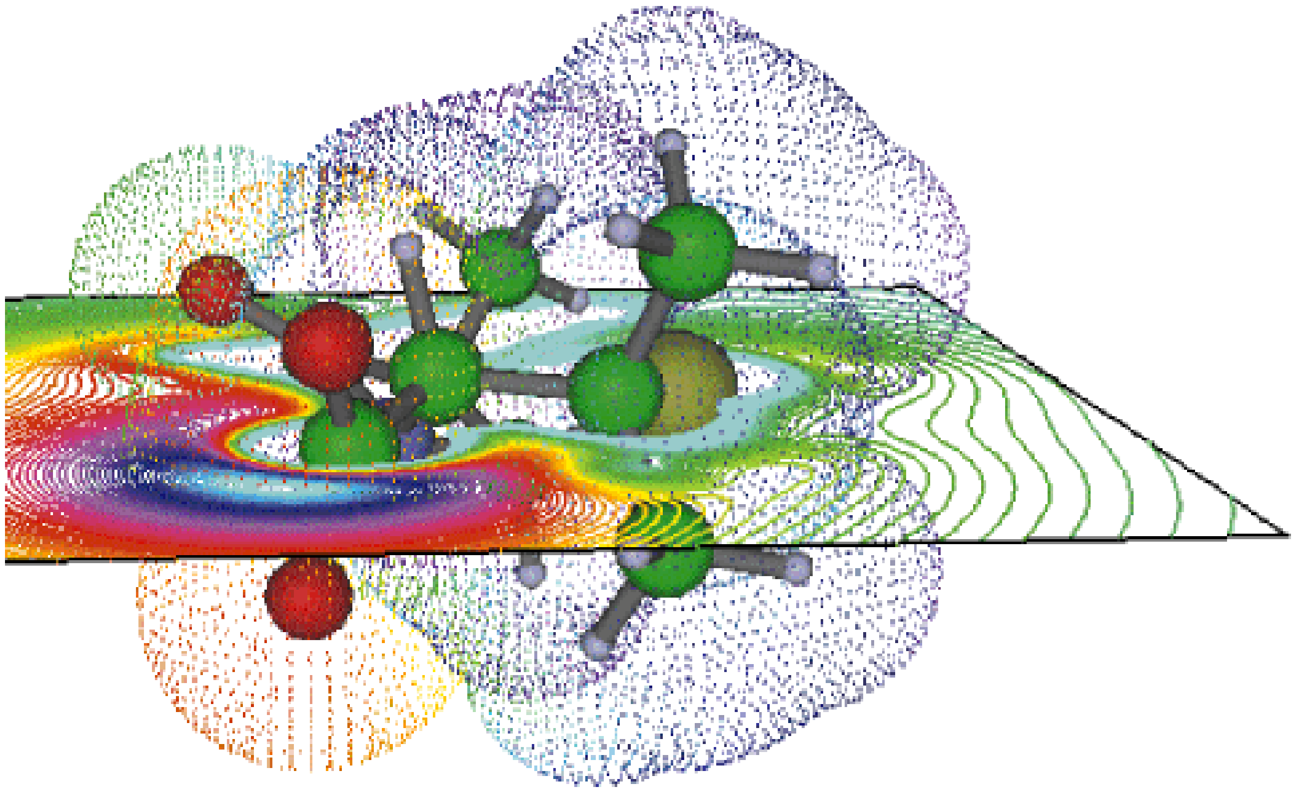
Potential Applications





Chemical-biological simulations, new drugs and materials, scientific research, cryptography, machine learning, big financial data.

Simulations

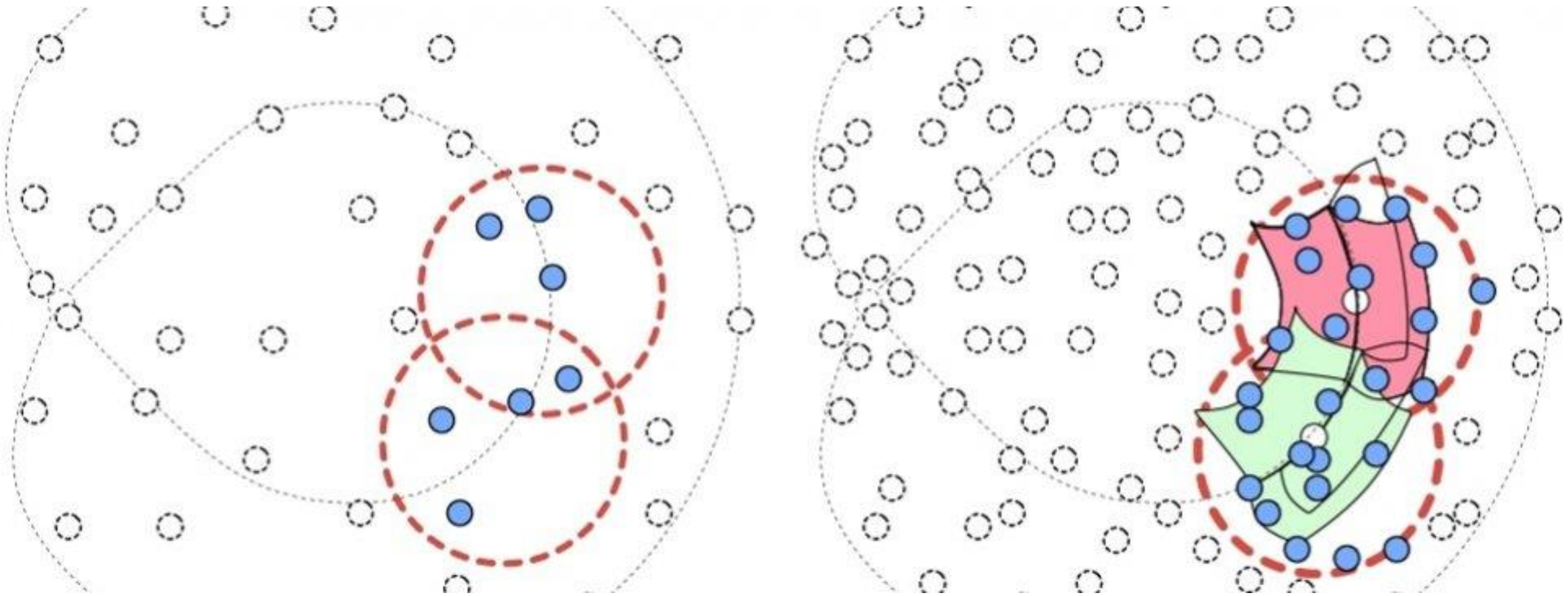


<u>Short run:</u> Potential use cases with (relatively) small number of qubits

Cryptoanalysis

<u>Long run:</u> Requires a wery large number of qubits

Machine Learning / AI



Long run: Research is in progress

Google / NASA Quantum AI Lab

Large Companies

Google
intel
Microsoft
IBM
LOCKHEED MARTIN
amazon
NVIDIA
BOEING
SIEMENS
Alibaba Group 阿里巴巴集团
NOMURA
J.P.Morgan

Large Companies: Examples 1

Google

- 72 qubit device, “Bristlecone“
- 100 People team
- 2 Hardware projects
- Estimated $ 0.5 Billion invested cumulatively
- Exploring both circuit and adiabatic models
- 10 Potential applications

Microsoft

- Hardware: “topological approach” with Majorana fermions - Long run view
- Software: building ad-hoc programming languages, potential short run applications

IBM

- Hardware: 53 qubit device + strong track record of reserach
- Software: building cloud / saas applications and developer tools

Large Companies: Examples 2

<u>Integration with cloud services:</u>

<We envision quantum computing being widely accessible as an integral part of the AWS Cloud so that all of our customers can benefit from it. Quantum computing, for instance, will increase the speed at which our customers can process complex scientific data in the cloud, which will enable unprecedented success in problem-solving, and supercharge research and development. >

Simone Severini as new «Director of Quantum» at Amazon Web Services

Startups: Examples – 1 | Full Stack | $+100M Funds

D:WAVE
The Quantum Computing Company™

- $ 205 M raised
- 180 Employees
- Sold devices to Nasa, Google, Lockeed, Wolkswagen, Los Alamos National Lab.
- Strong IP portfolio
- Investors group includes DJF, Goldman Sachs, Bezos Expeditions, Fidelity
- Government/Defense support
- Controversial adiabatic approach
- Issues: non-universal devices (only specific functions), no error correction.

rigetti

- $ 120 M raised
- 144 Employees
- Investors goup includes Andresseen Horowitz, Funders Fund, Y Combinator, Bloomberg Beta
- Building 50 qubit device
- Circuit approach
- Quantum chemistry team

Startups: Examples – 2 | Hardware

IONQ

Quantum Circuits

PsiQ

- $ 75 M Funding (Google Ventures, NEA)
- Ion-trap based Hardware

- $ 18 M raised
- Superconducting devices / Electronics for quantum computers

- $230 M raised
- Photonic approach

Startups: Examples – 3 | Software

CAMBRIDGE QUANTUM COMPUTING LIMITED

- $ 50 M Funding (Ilyas Kahn)
- Software solutions / Operating Systems

ZAPATA

- $ 31,4 M raised
- Quantum Software

XANADU

- $ 35,6 M from OMERS, Golden Ventures and Real Ventures.
- 32 Employees
- Hardware: Silicon photonic chips with Qumodes - Pro: scalability
- Software: Focus on Simulations & Machine learning applications

1QBit

- $ 50 M raised – 85 people
- B2B Software – Simulations
- APIs, SDKs, algos
- Existing clients: Accenture, Fujitsu

Investors

G/

Y Combinator

Goldman Sachs

ANDREESSEN HOROWITZ

DFJ

NEA®

FOUNDERS FUND

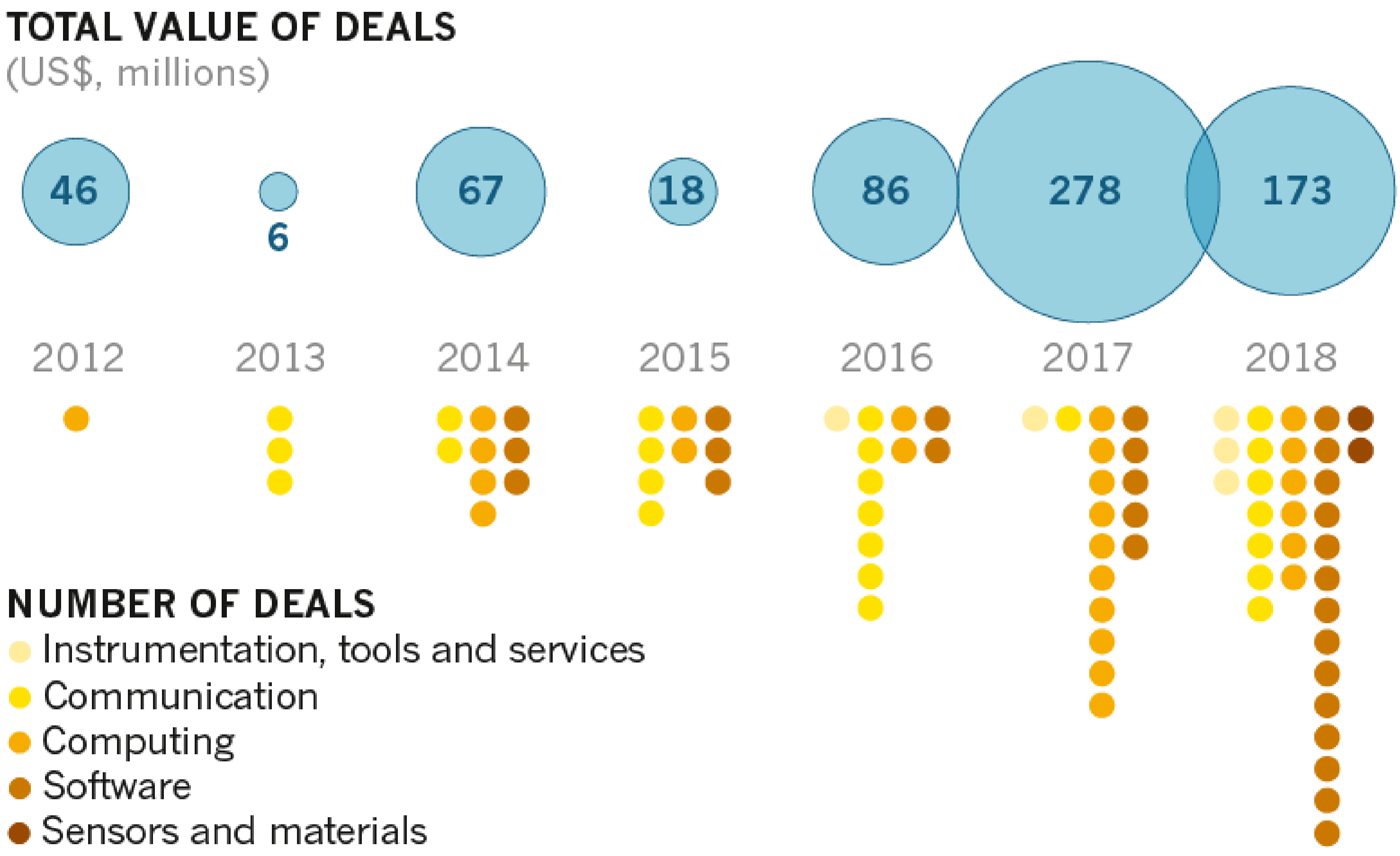
Blue Yard

Redpoint VENTURES

BEZOS EXPEDITIONS

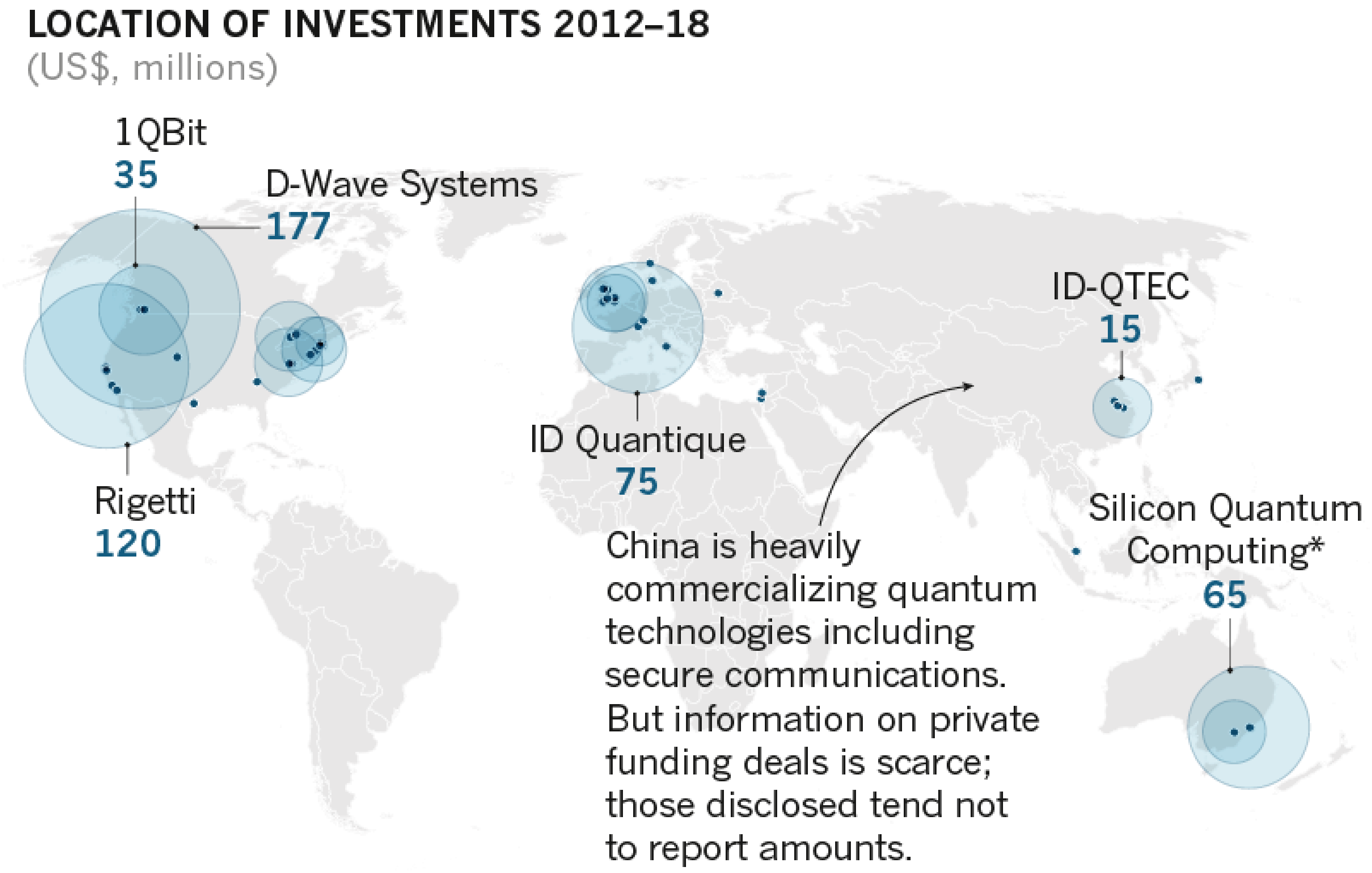
IQT® IN-Q-TEL

VC investments in quantum tech companies - 1



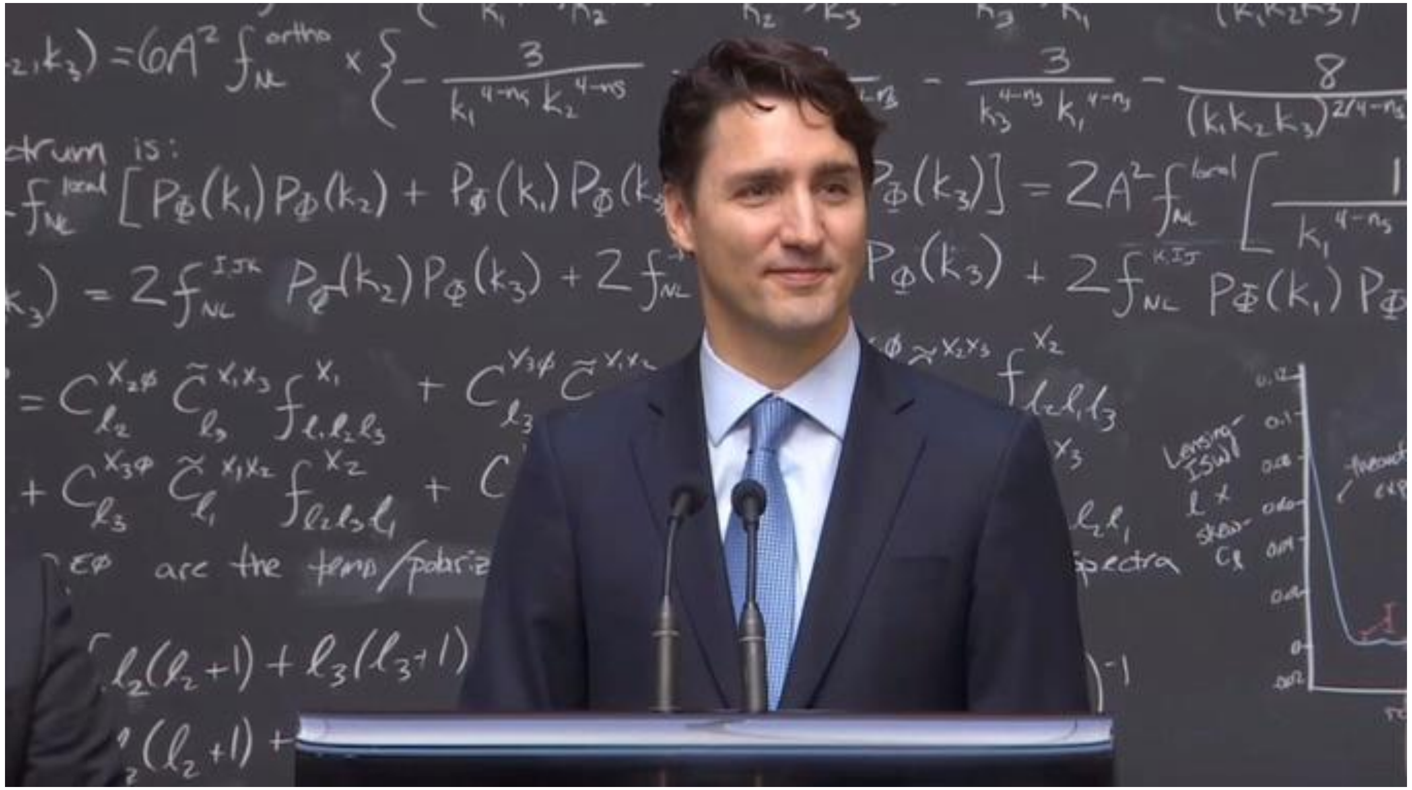
Source: Nature

VC investments in quantum tech companies - 2

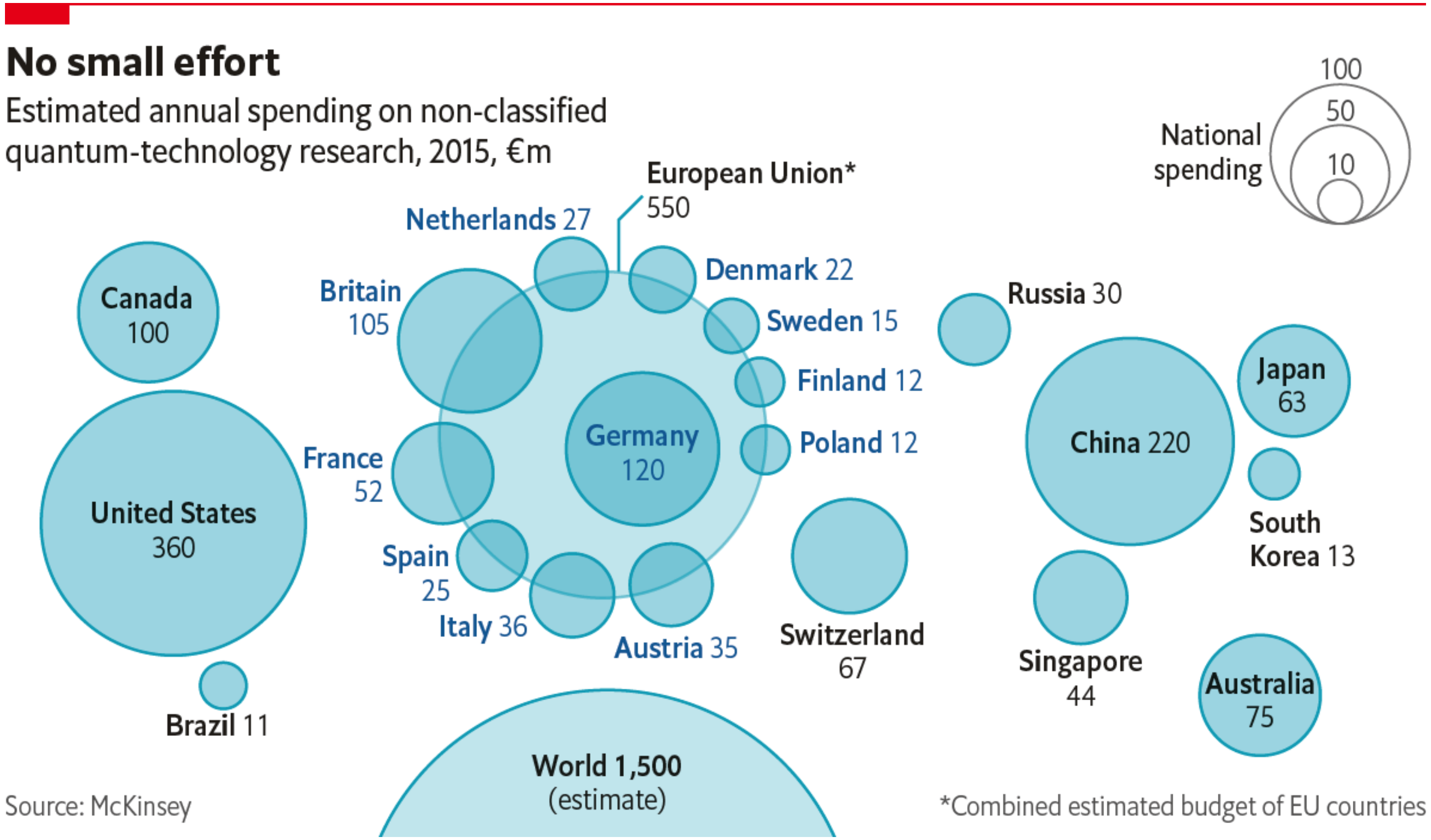


Source: Nature

Political Hype

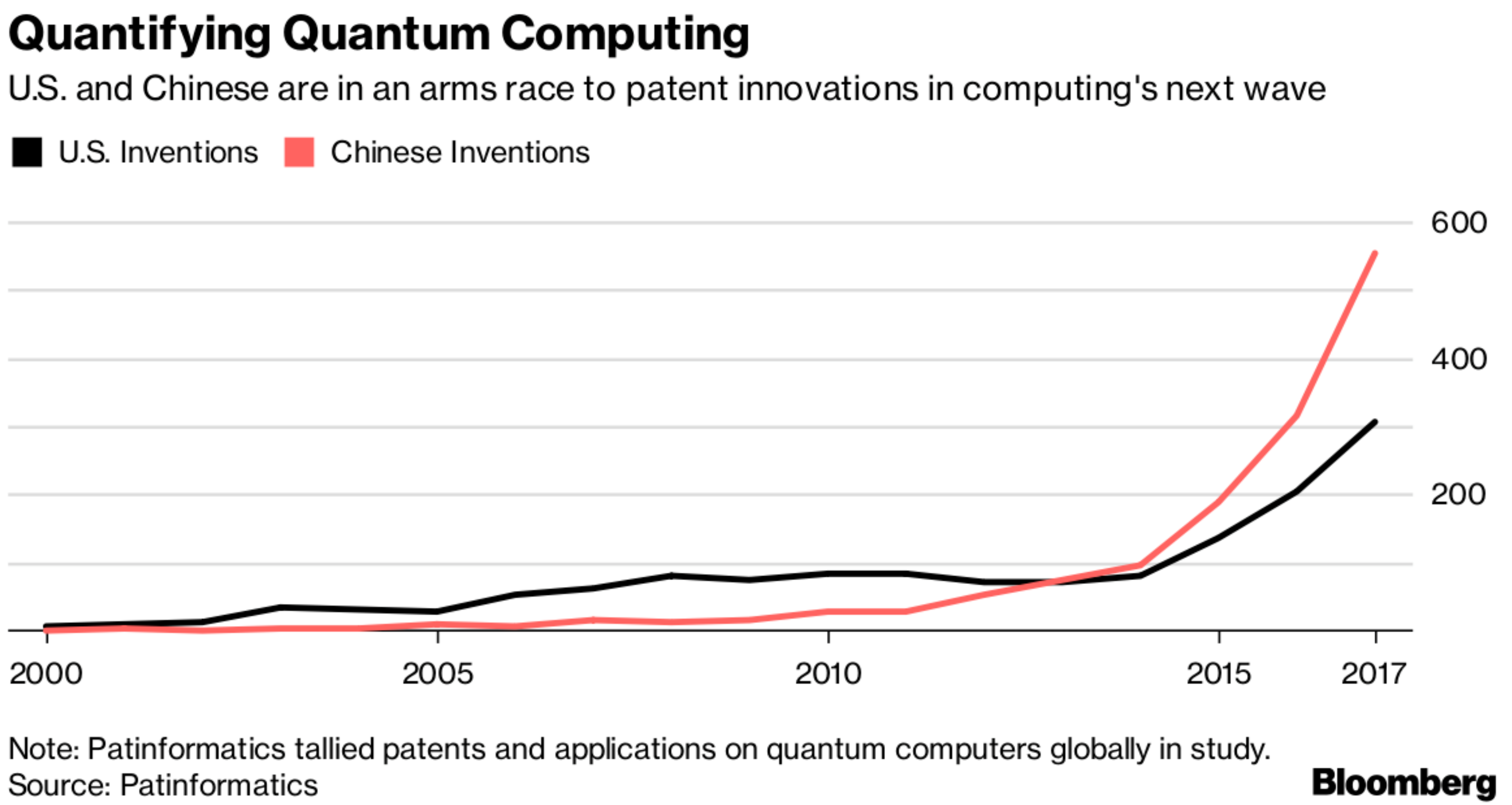


Government Programs



Sources: The Economist, McKinsey

China: Rising innovation performance



China is building a $ 10 Bn quantum applications research centre

$ 3 Bn allocated to quantum computing

US National Quantum Initiative Act

$ 1.3 Bn allocated + National Quantum Coordination Office

European Union:
Technology Flagship Program - € 1 Bn

Intelligence and Defense

Resources

APIs / SDKs

Quantum Computing Playground
http://www.quantumplayground.net/

Quantum Composer and QISKit software developer kit
https://quantumexperience.ng.bluemix.net

LIQUi|> is a software architecture and toolsuite for quantum computing
http://stationq.github.io/Liquid/

Forest and pyQuil:
Quantum programming in Python
https://www.rigetti.com/forest

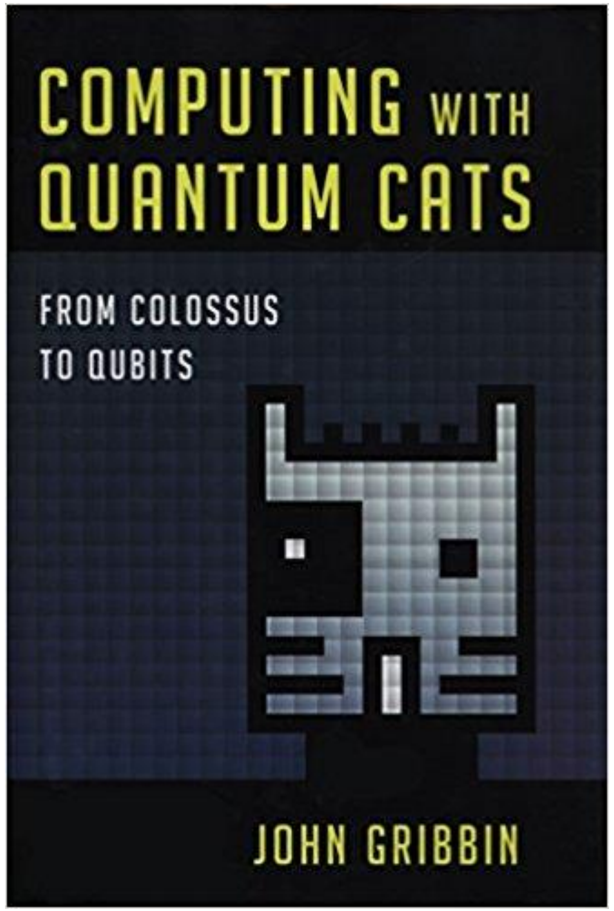
Open Source

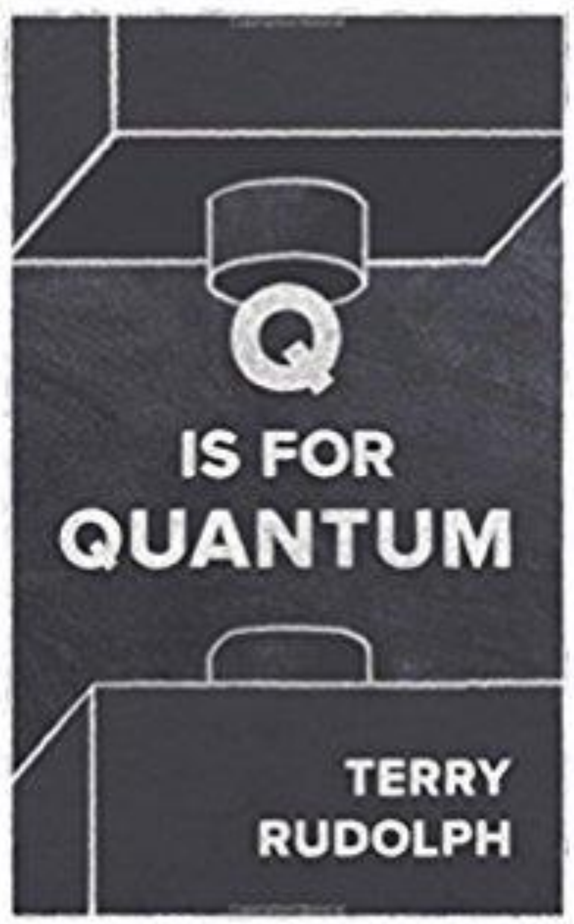
QuTiP

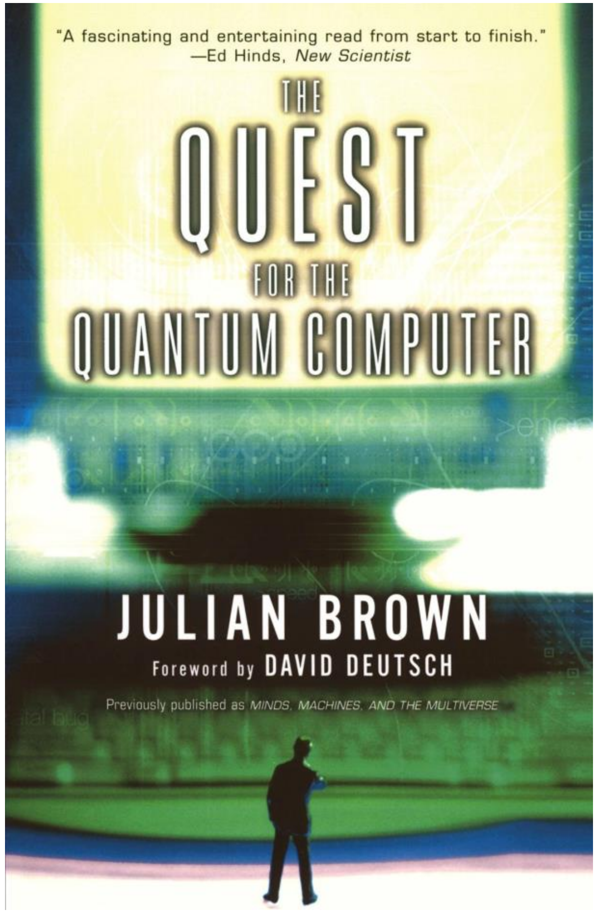
Quantum Toolbox in Python

QuTiP is open-source software for simulating the dynamics of open quantum systems.
http://qutip.org/

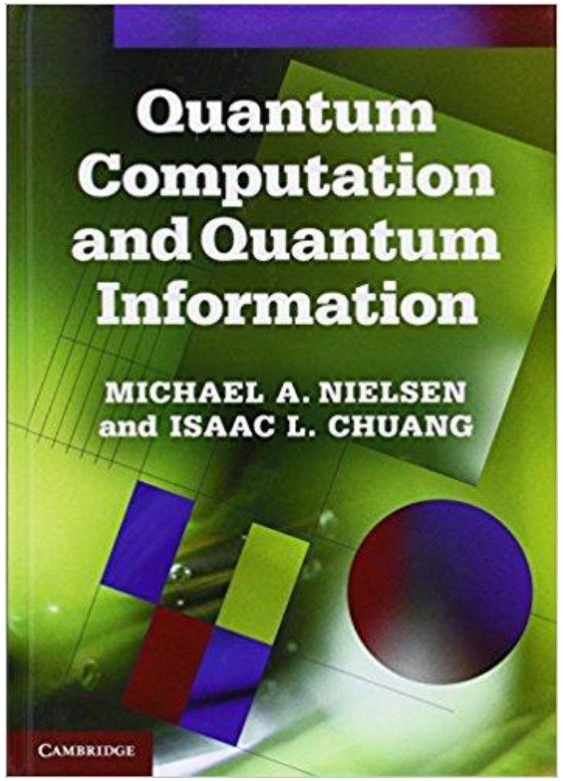
Books a) -> Popular Science / Mainstream Media

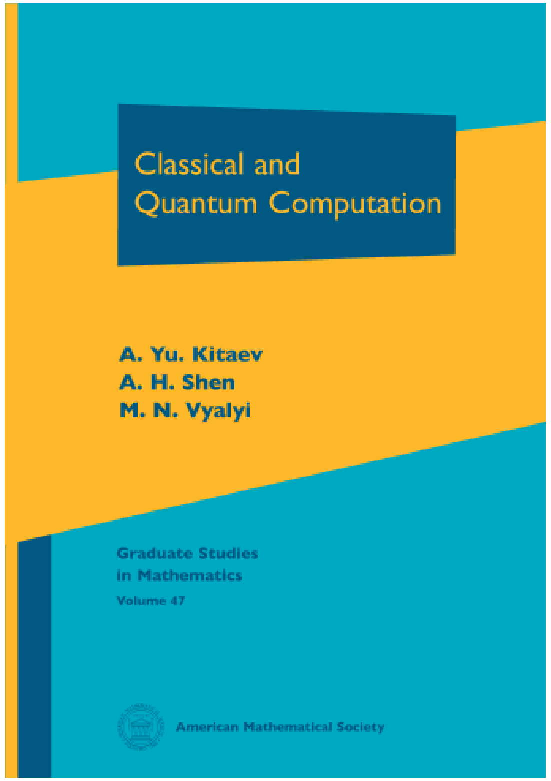


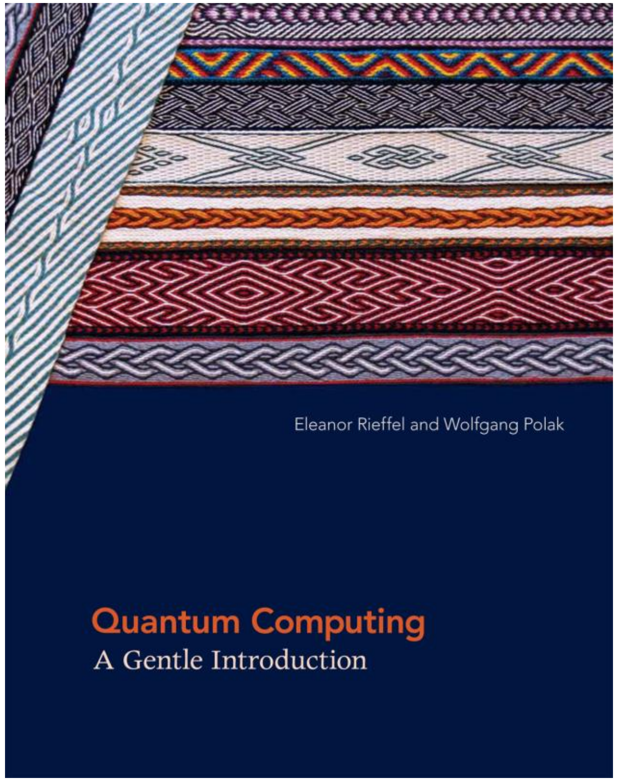




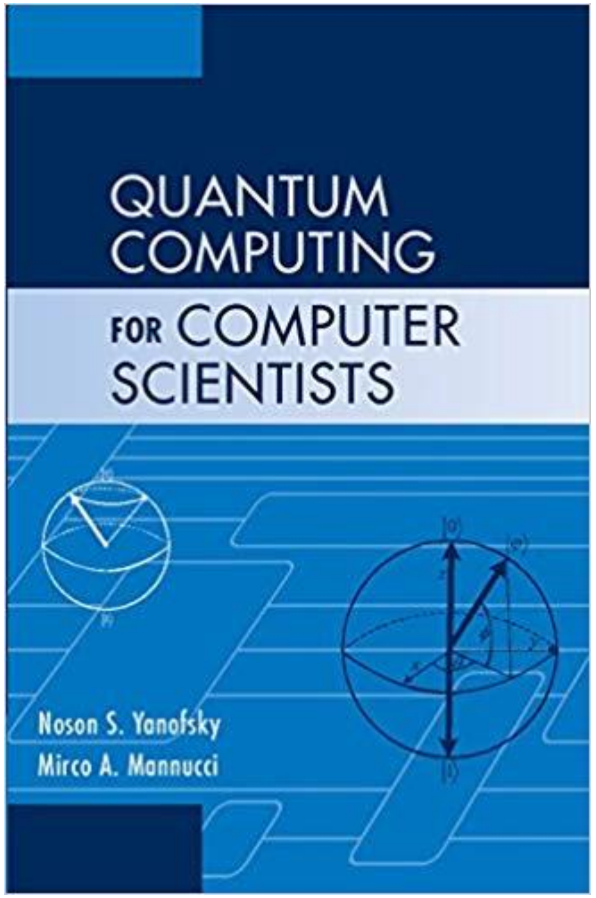
Books b) -> Technical Books

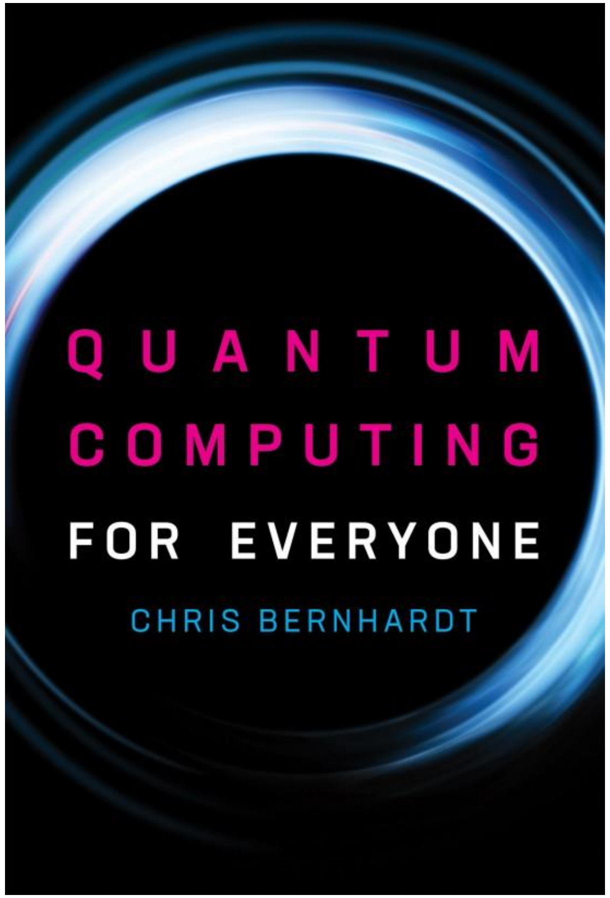




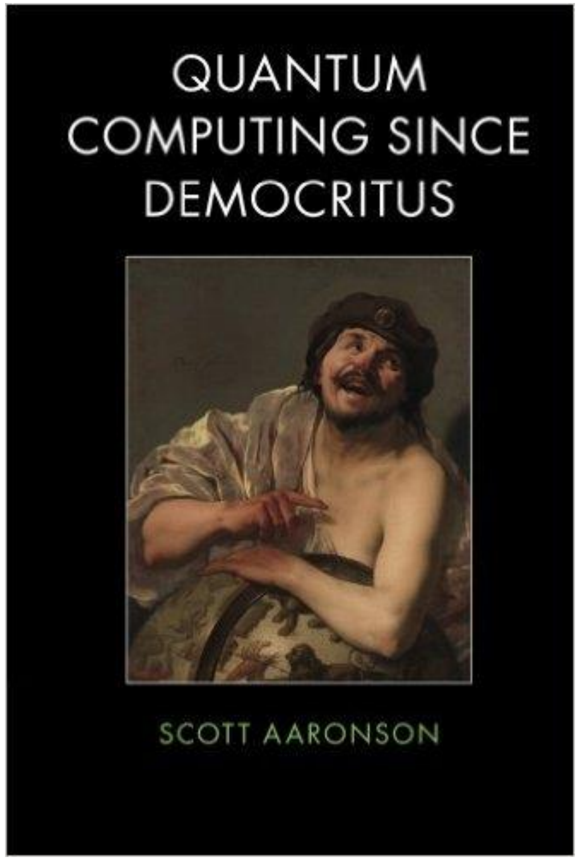


Books c) -> Semi-Technical Books



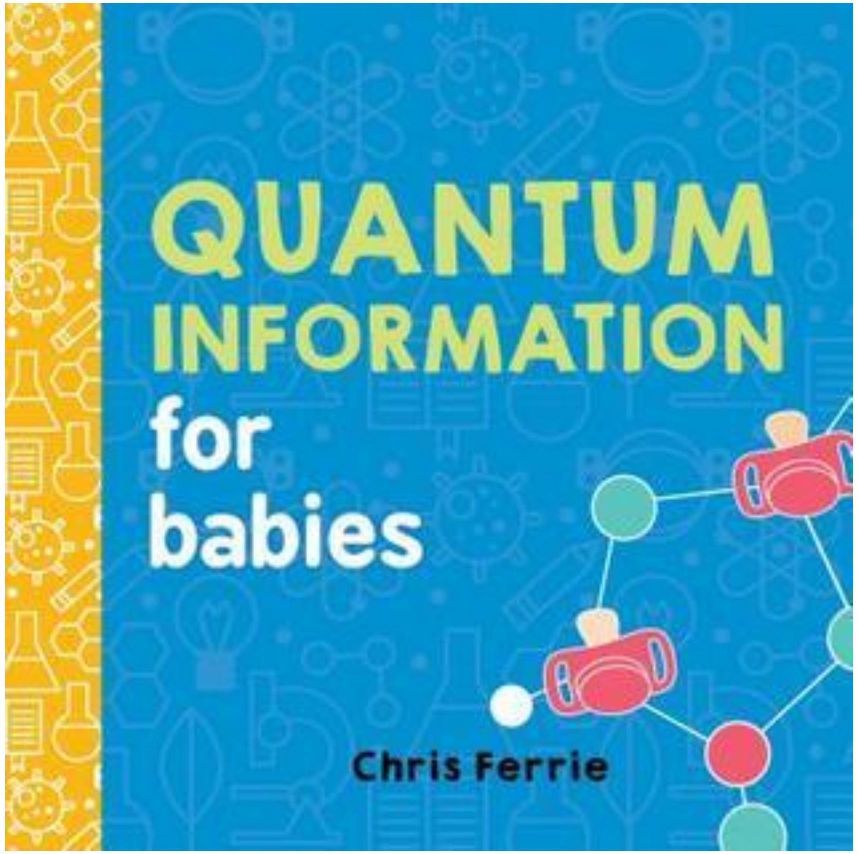


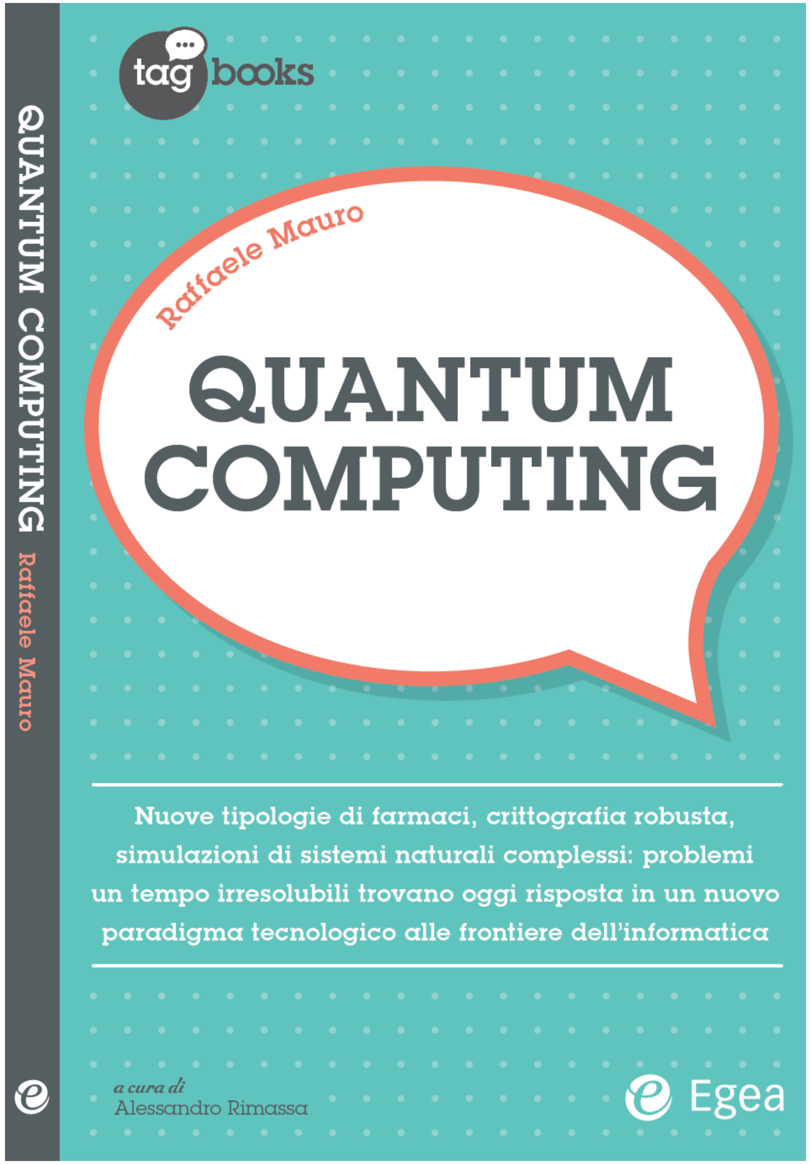
Books d) -> High Level Analysis



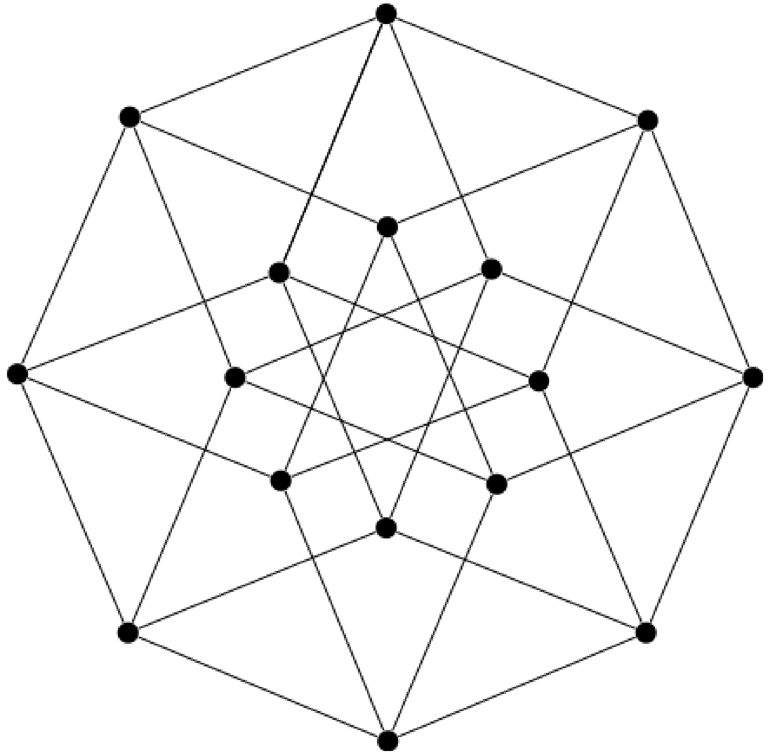
"A candidate for the weirdest book ever published by Cambridge University Press" (cit.)

Books e) -> Baby Books !




tag books
Raffaele Mauro
QUANTUM COMPUTING
Nuove tipologie di farmaci, crittografia robusta, simulazioni di sistemi naturali complessi: problemi un tempo irresolubili trovano oggi risposta in un nuovo paradigma tecnologico alle frontiere dell'informatica
a cura di
Alessandro Rimassa
Egea
QUANTUM COMPUTING Raffaele Mauro

Thank you !



raffaele.mauro@endeavor.org

Raffaele Mauro, Ph.D.

Raffaele Mauro is passionate about technology, policy and global finance.

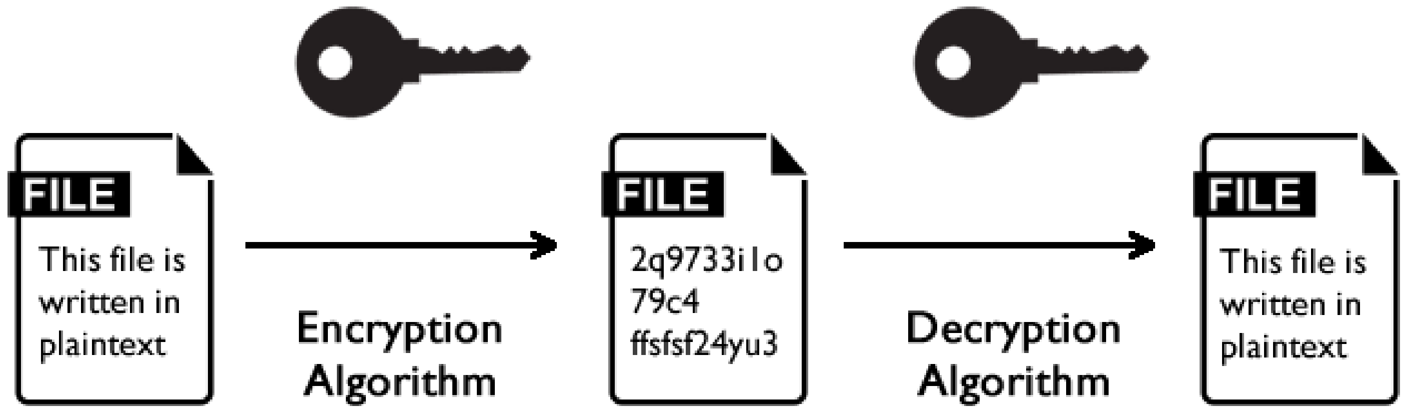
Now Managing Director at Endeavor Italy, he is focused on high-impact entrepreneurship and venture capital, providing companies access to smart capital, talent and markets. Previously he was Head of Finance for Innovation & Entrepreneurship at Intesa Sanpaolo and worked at venture capital funds such as United Ventures (formerly Annapurna Ventures), P101 and OltreVenture.

Raffaele is a Kauffman Fellow and holds an MPA from Harvard University, a Ph.D. from Bocconi and is alumnus of the Singularity University Graduate Studies Program at NASA Ames. Raffaele co-authored the book “Hacking Finance”, an essay on Bitcoin, blockchain and cryptocurrencies, and was invited speaker at EY EMEIA Accelerate, Wired Money and the Bundesbank.

Raffaele is also Junior Fellow at the Aspen Institute, member of the Young Leaders group of the US-Italy Council, member of the “Young European Leaders – 40 under 40” cohort of 2011 and member of the executive committee at the Global Shapers Hub - Milano, a World Economic Forum community.

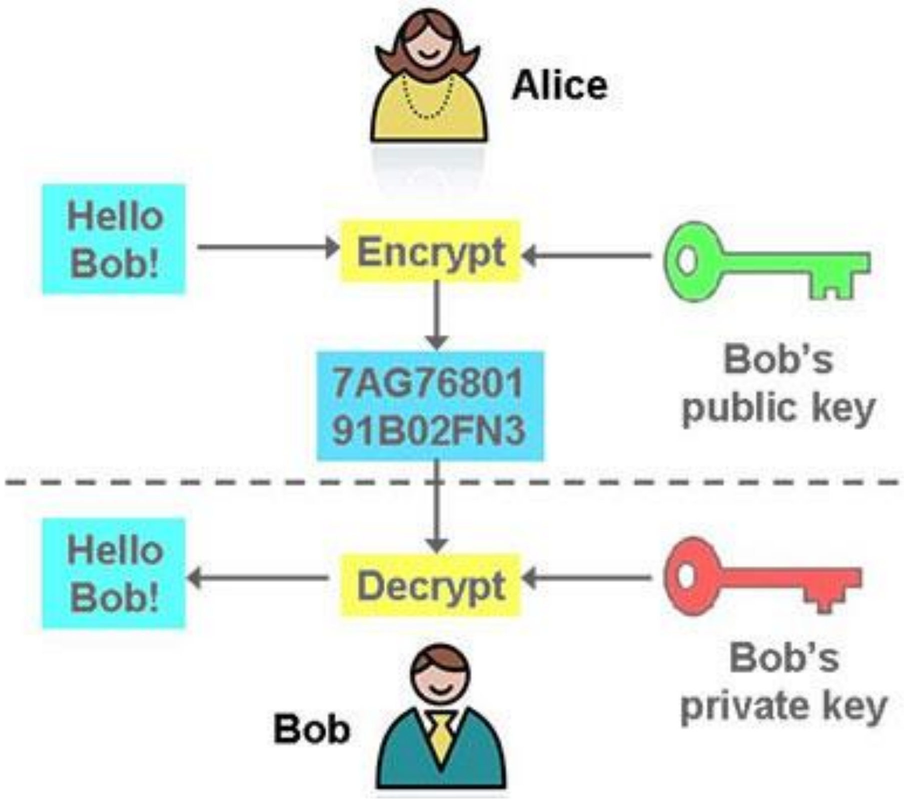
Twitter: @rafr

The Mathematics of Secrets: Symmetric cryptography



Issue: Key distribution - third party could intercept keys

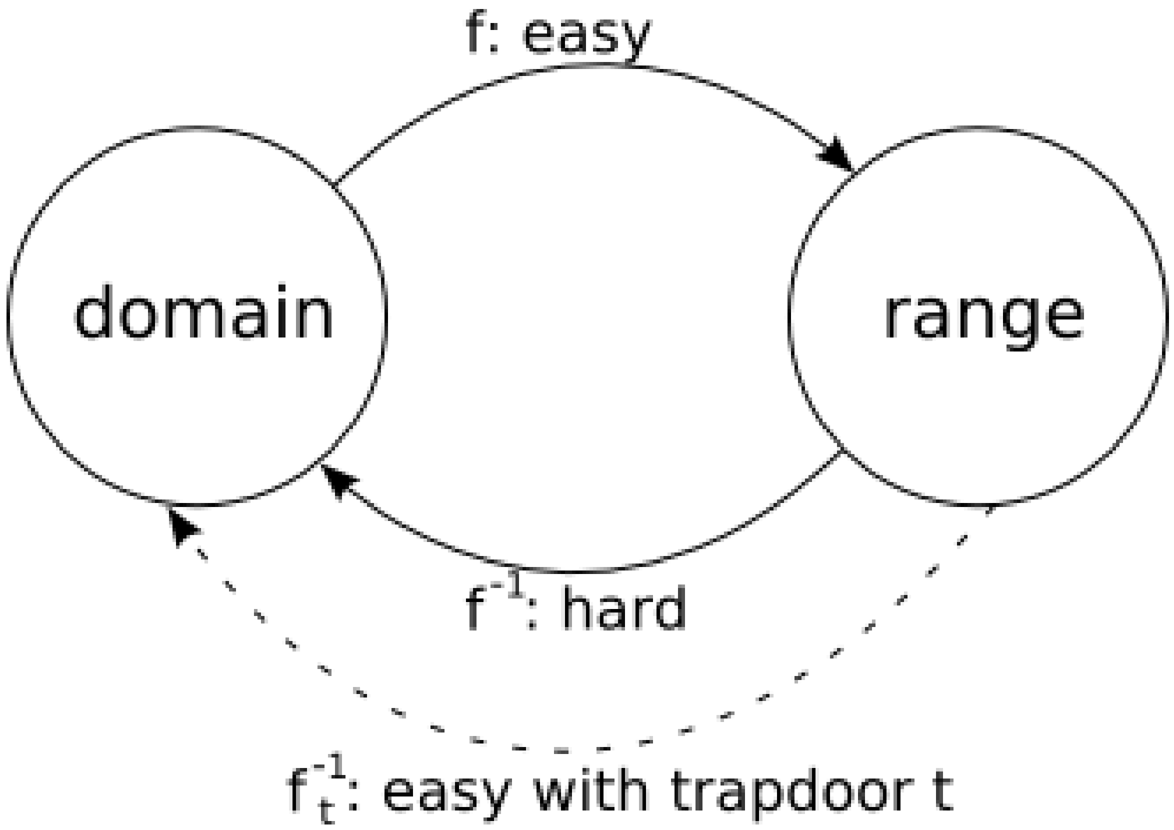
Public Key / Asymmetric Cryptography



<u>Issue:</u> Key generation - key size and "quality" / randomness

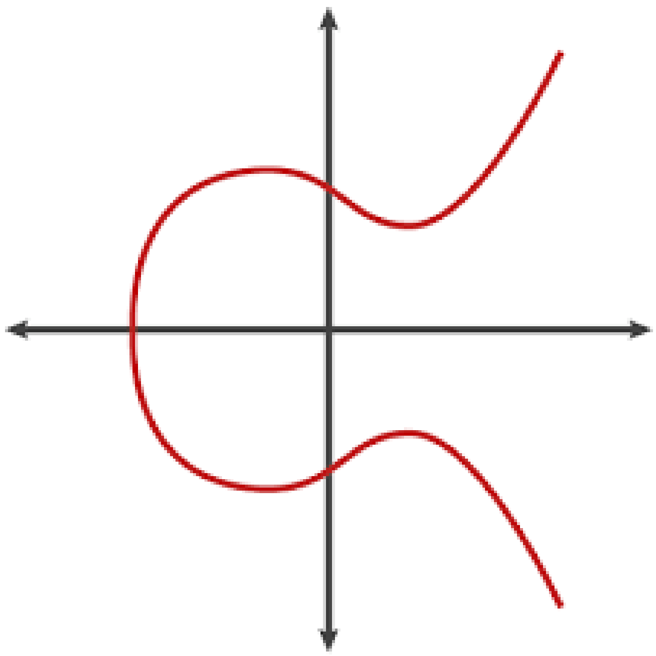
Otherwise private key deductible from public key

Trapdoor / Unidirectional functions



Example: RSA Algorithm, public key from large prime number multiplication

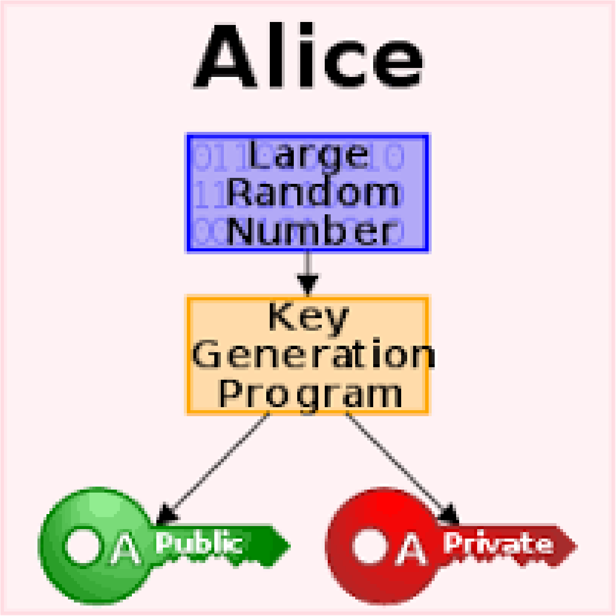
Elliptic Curve Digital Signature Algorithm (ECDSA)

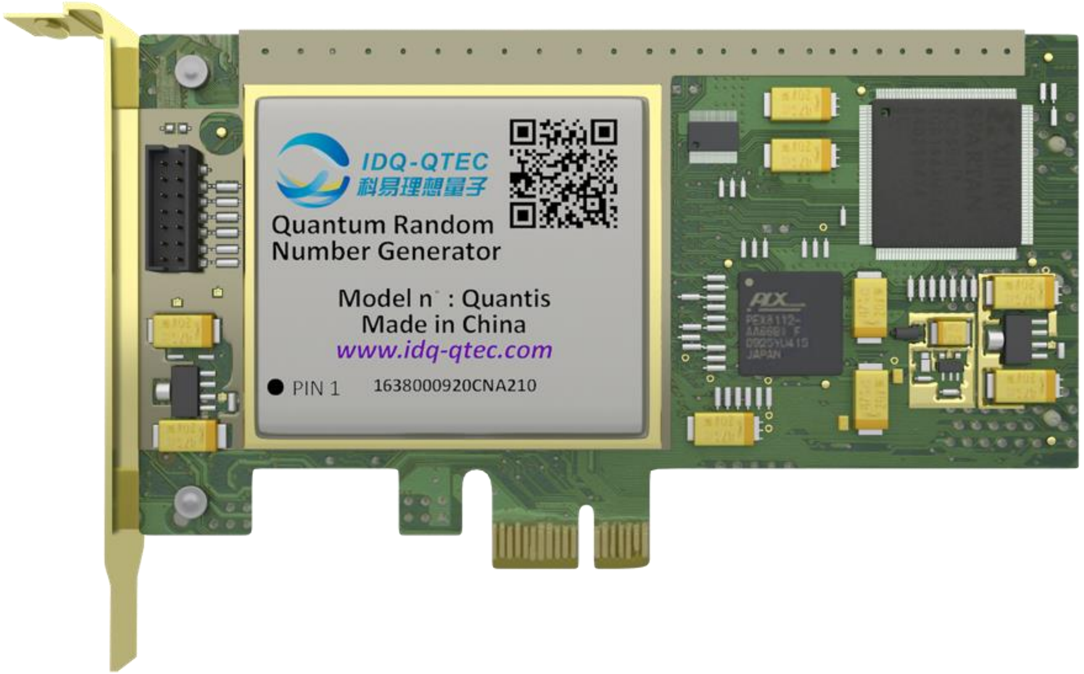


Cubic curves –> Discrete logarithm function is unidirectional

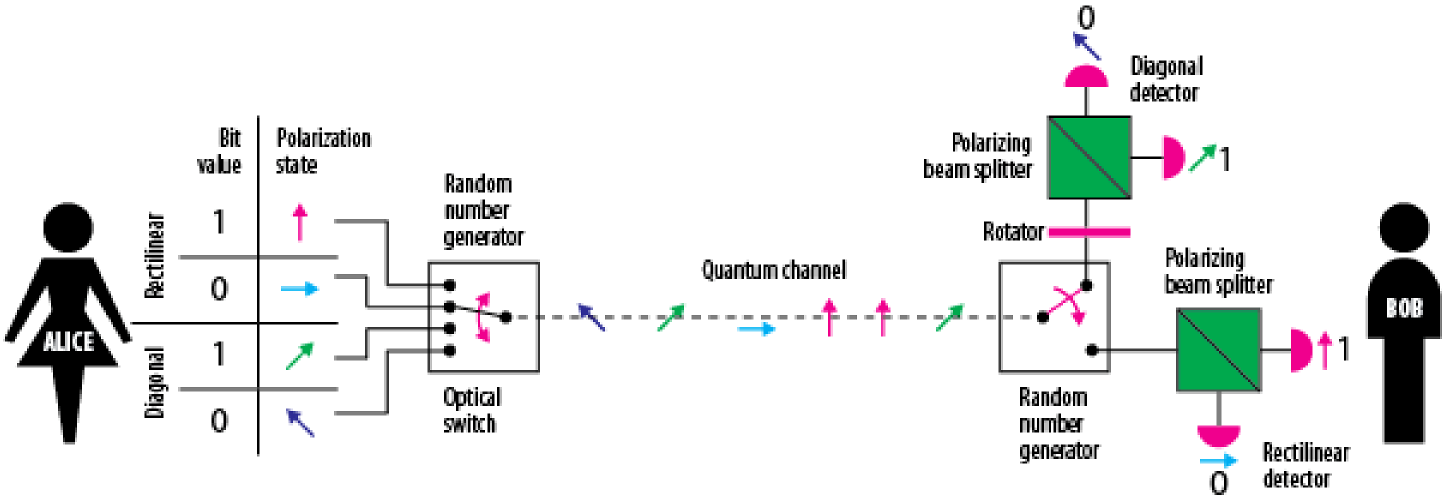
Higher security with shorter keys, SHA-256

Quantum Random Number Generation





Quantum Key Distribution



Quantum transmission & detection	ALICE sends photons	↖	↗	→	↑	↑	↗	↖	↑
	ALICE's random bits	0	1	0	1	1	1	0	1
	BOB's detection events	↑	↗	↖	↑	↗	↗	↖	↖
	BOB's detected bit values	1	1	0	1	1	1	0	0
Public discussion (i.e., sifting)	BOB tells ALICE the basis choices he made	Rect	Diag	Diag	Rect	Diag	Diag	Diag	Diag
	ALICE tells BOB which bits to keep		✔		✔		✔	✔	
	ALICE and BOB's shared sifted key	–	1	–	1	–	1	0	–

Micius Satellite: quantum entanglement & secure communication