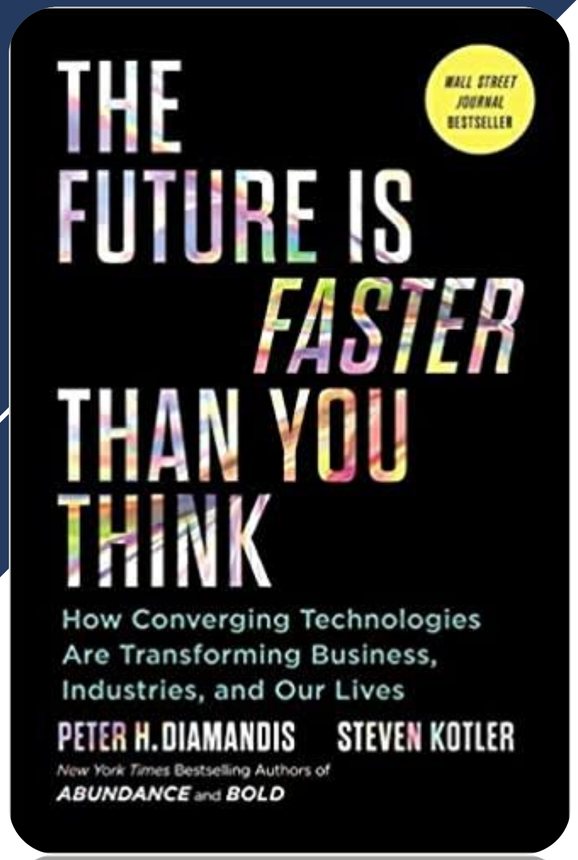
Uso de Tecnologias Quânticas e seus Impactos Futuros

Regina Melo Silveira
Waldemir Cambiucci

LARC- Laboratório de Arquitetura e Redes de Computadores
Escola Politécnica da Universidade de São Paulo
regina@larc.usp.br

Agenda



A Computação Quântica

Características quânticas, qubits, as evoluções alcançadas e aplicações

Consequências da CQ

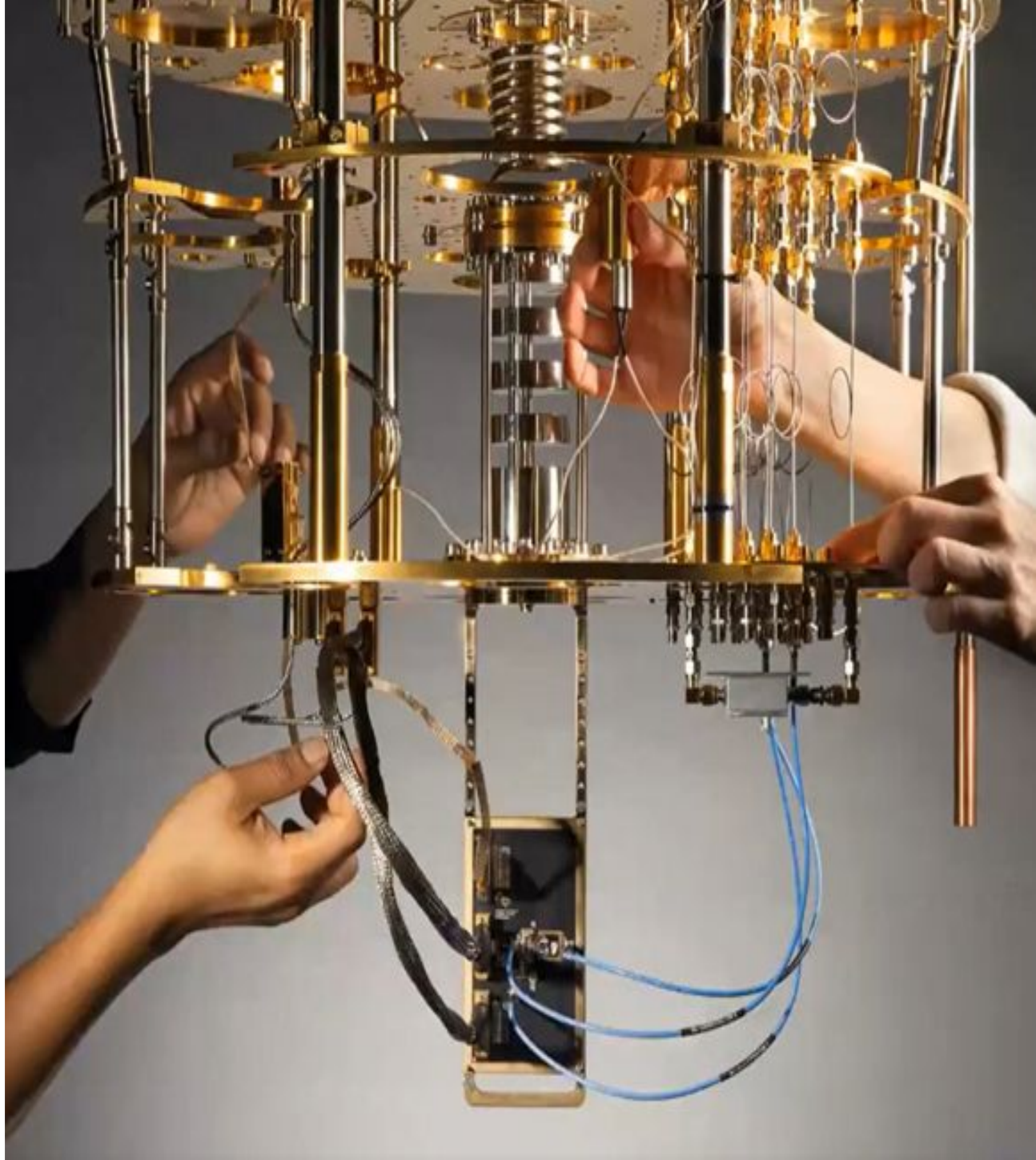
Criptografia Pós-Quântica

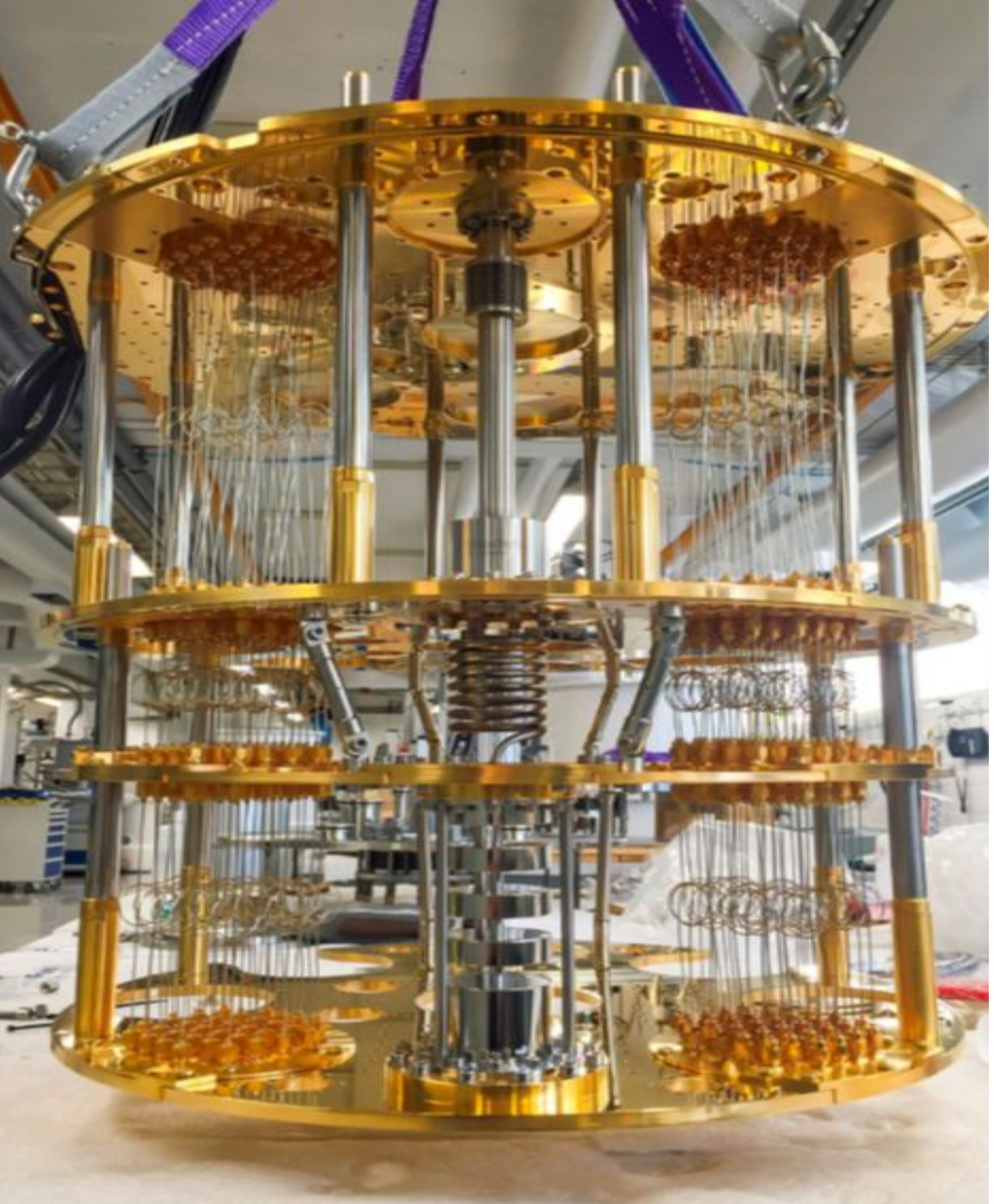
Internet Quântica

Evolução e expectativas

Cenários de uso, investimentos e mercados em potencial

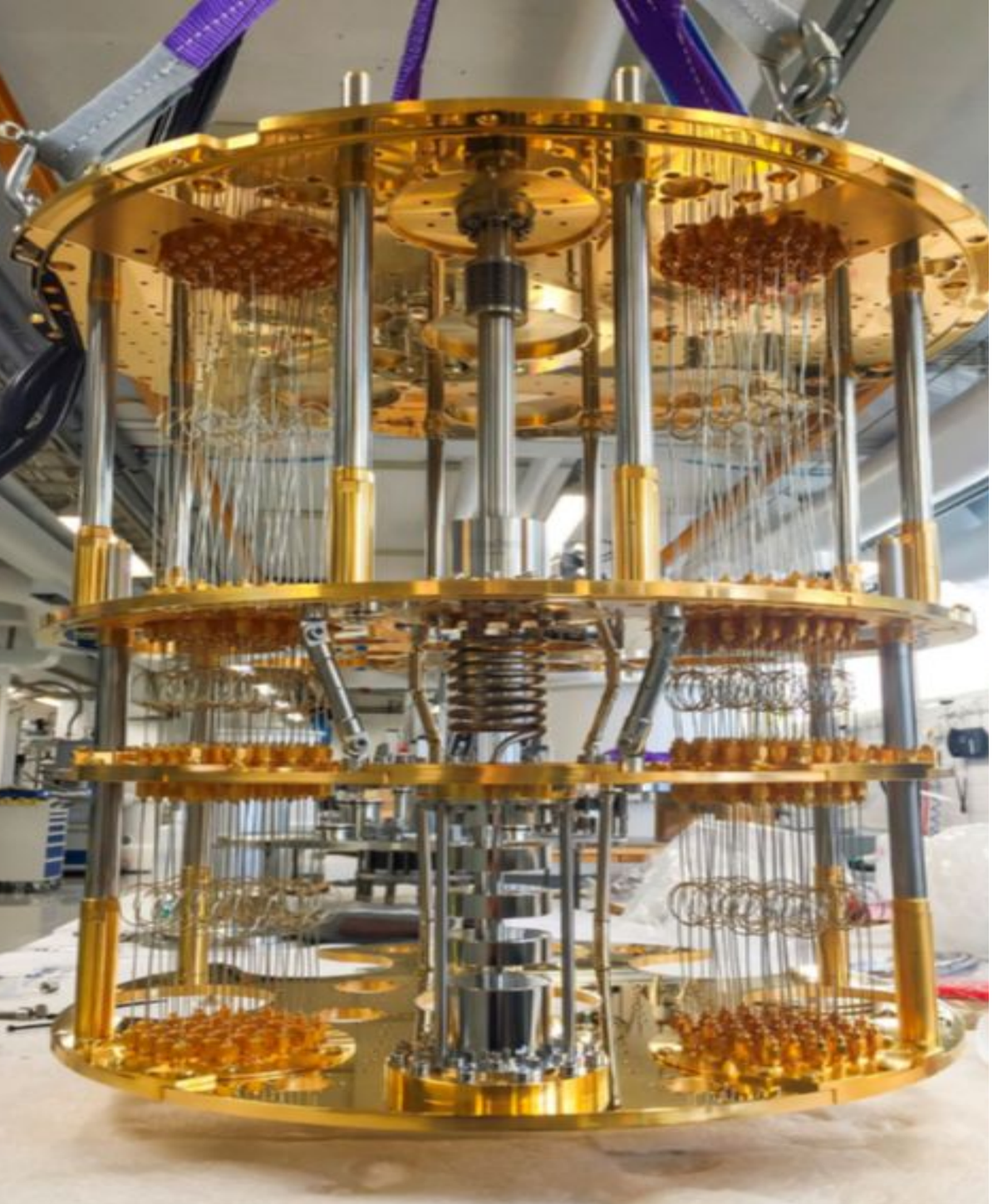
O que é Computação Quântica?





O que é Computação Quântica?

É um novo **modelo computacional** baseado em **princípios da mecânica quântica**, que pode resolver problemas muito complexos para computadores clássicos.



O que são computadores quânticos?

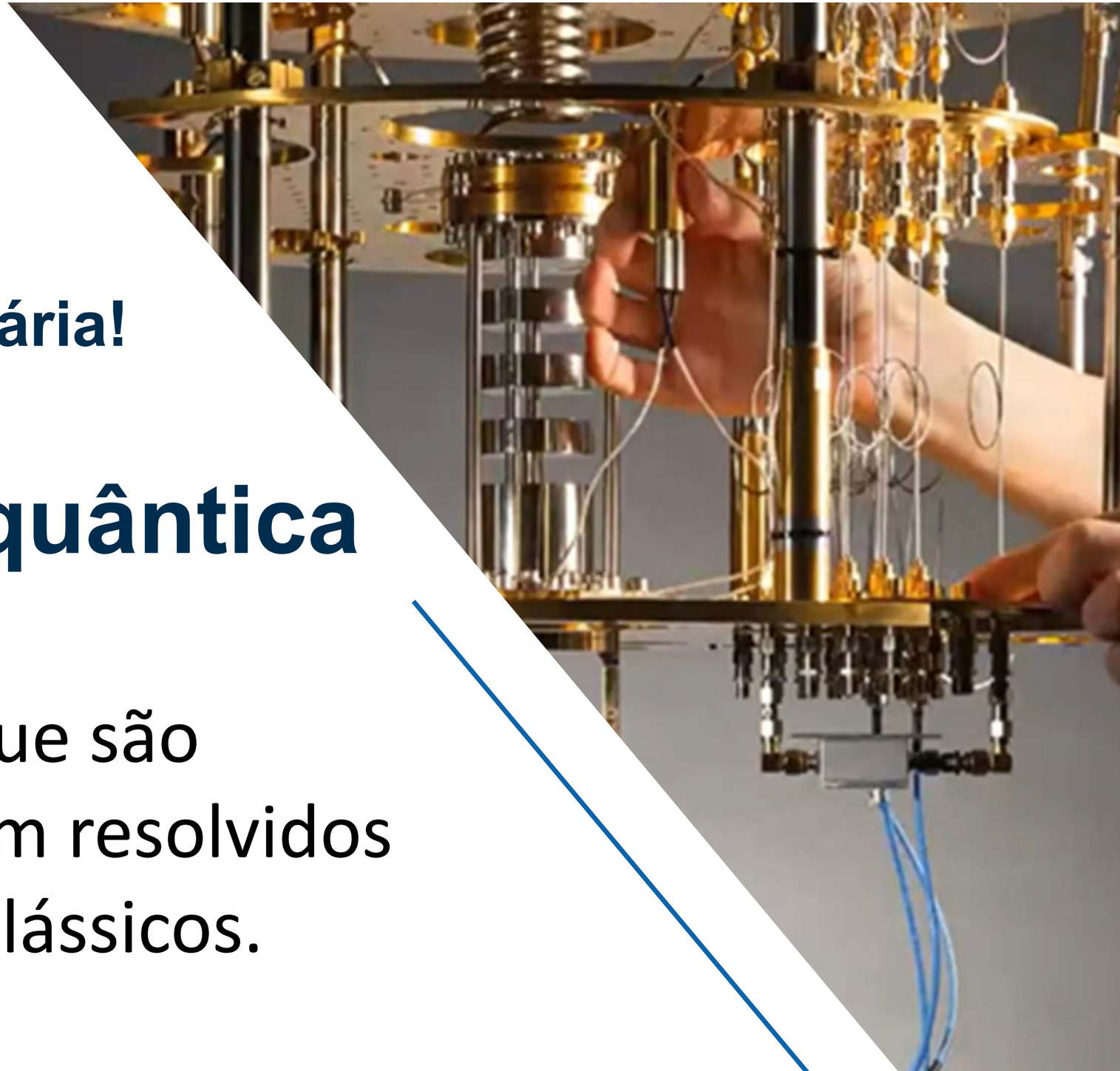
Uma nova geração de **máquinas de resolução de problemas**.

Não são menores, mais rápidos ou melhores – eles operam sob **um novo paradigma!**

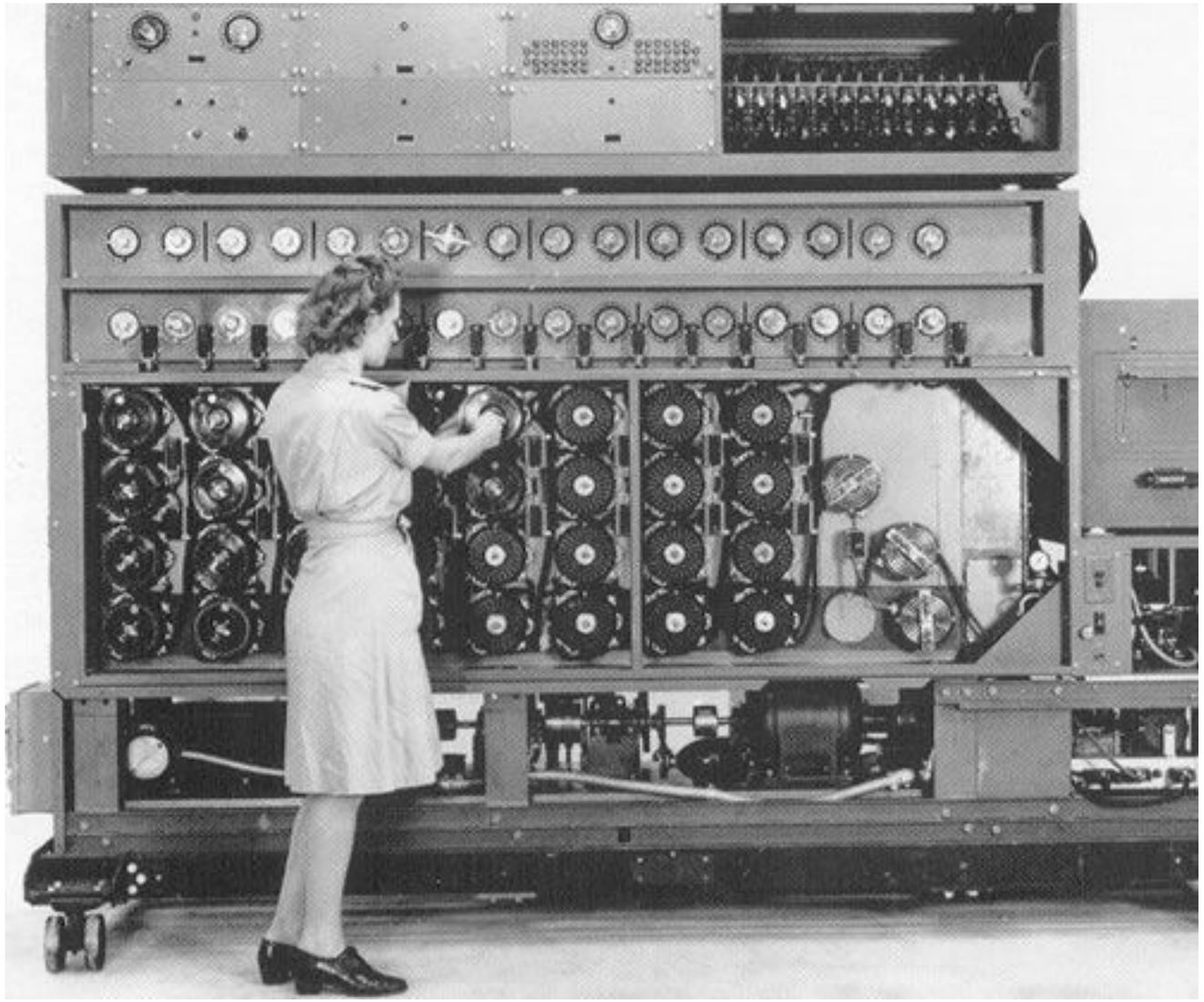
A Natureza não é binária!

A Natureza é quântica

Temos problemas que são impossíveis de serem resolvidos em computadores clássicos.



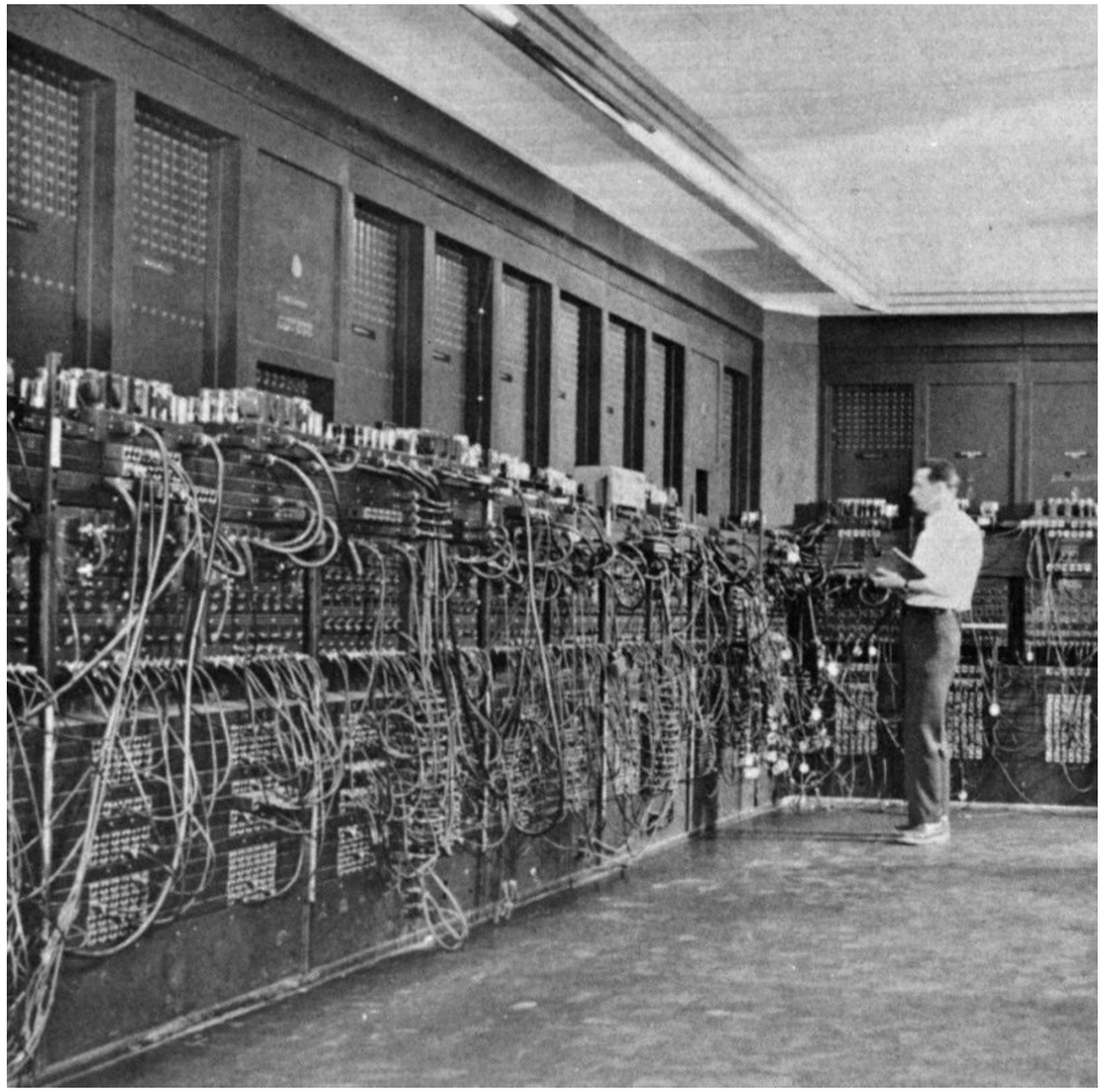
Computadores clássicos são baseados em estados binários



“On Computable Numbers”, Alan Turing, 1939

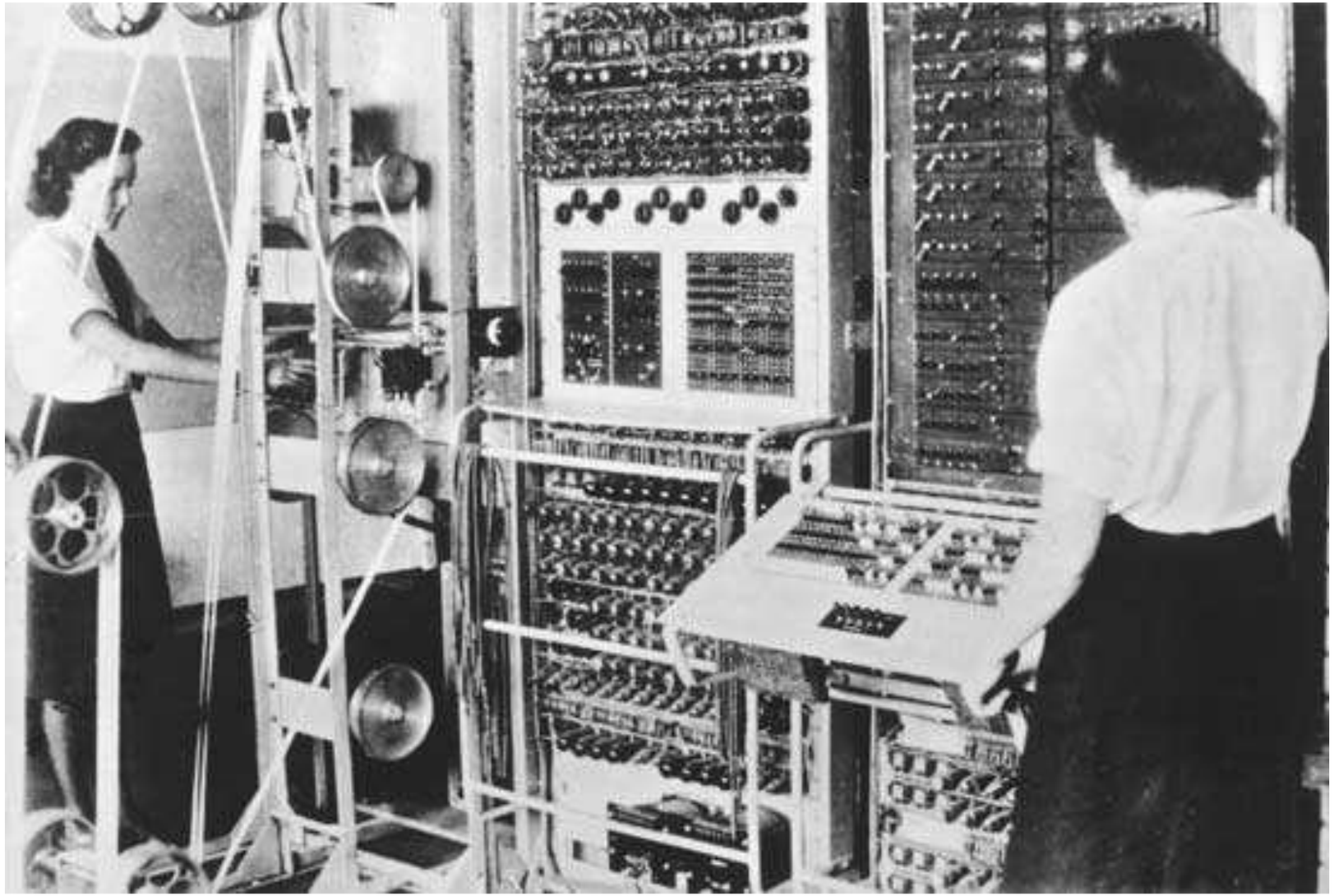
ENIAC (1946)

- Zeros e Uns



Computadores clássicos são baseados em estados binários

Grande evolução nos últimos 80 anos



Colossus, the first large-scale electronic computer, which went into operation in 1944 at Britain's wartime code-breaking **headquarters at Bletchley Park**

Richard Feynman

Richard Phillips Feynman was an American theoretical physicist, Nobel Prize in Physics in 1965

The Physics of Computation seminars , Caltech (1981)

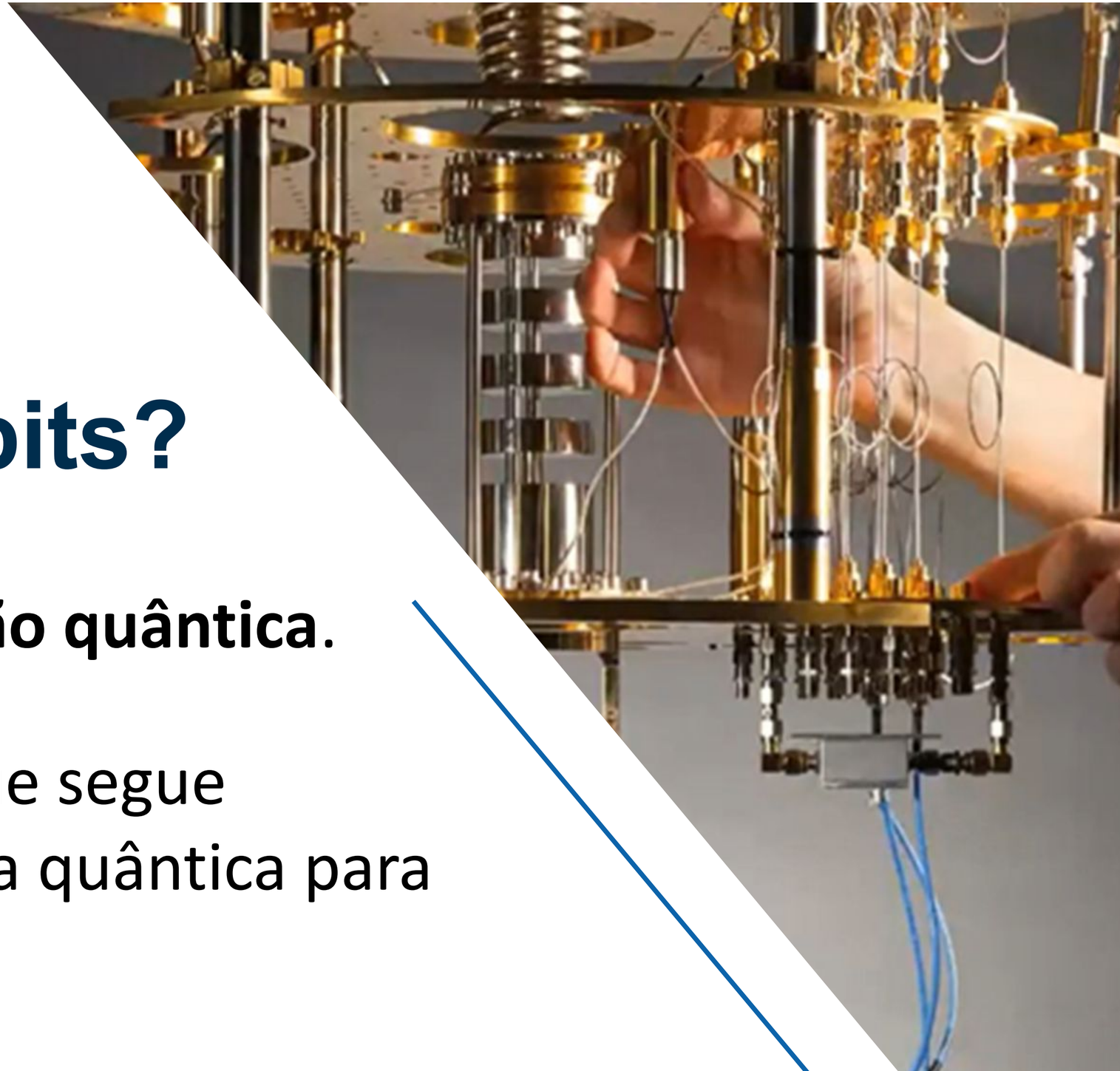
Now I explicitly go to the question of how we can simulate with a computer—a universal automaton or something—the quantum-mechanical effects. (The usual formulation is that quantum mechanics has some sort of a differential equation for a function ψ.) If you have a single particle, ψ is a function of x and t, and this differential equation could be simulated just like my probabilistic equation was before. That would be all right and one has seen people make little computers which simulate the Schröedinger equation for a single particle. But the full description of quantum mechanics for a large system with R particles is given by a function $\psi(x_1, x_2, \ldots, x_R, t)$ which we call the amplitude to find the particles $x_1, \ldots, x_R$, and therefore, because it has too many variables, it *cannot be simulated* with a normal computer with a number of elements proportional to R or proportional to N. We had the same troubles with the probability in classical physics. And therefore, the problem is, how can we simulate the quantum mechanics? There are two ways that we can go about it. We can give up on our rule about what the computer was, we can say: Let the computer itself be built of quantum mechanical elements which obey quantum mechanical laws. Or we can turn the other way and say: Let the computer still be the same kind that we thought of before—a logical, universal automaton; can we imitate this situation? And I'm going to separate my talk here, for it branches into two parts.

*"Let´s build computers based in **quantum mechanical elements**, which obey **quantum mechanical laws**!"*

O que são qubits?

Unidade de **informação quântica**.

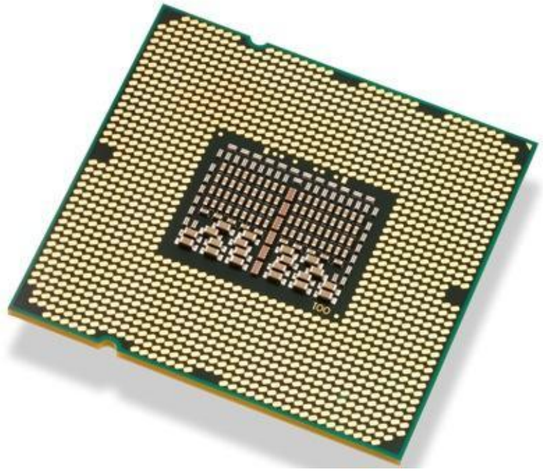
Precisamos de algo que segue princípios de mecânica quântica para realizar um qubit!



O que é um bit clássico?

switch

transistor



CPU

Datacenter

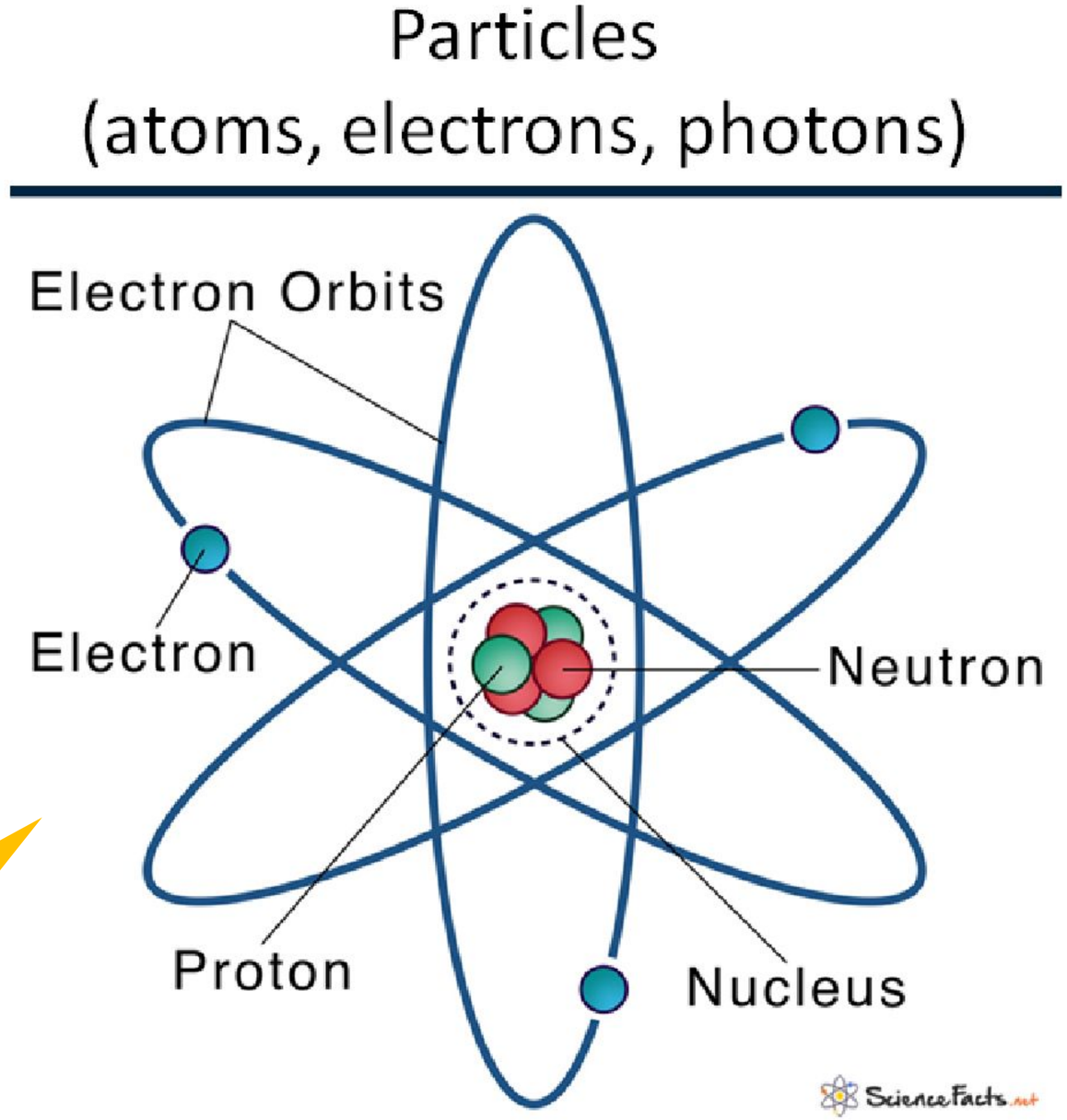
`0 ou 1`

`Ele é binário!`

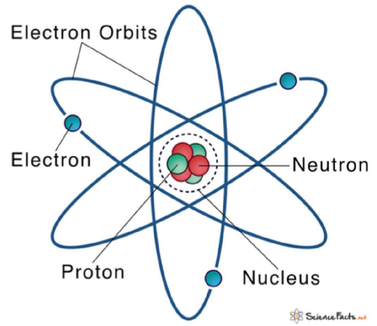
O que é um qubit ou quantum bit?

Preciso de alguma coisa que siga princípios de mecânica quântica!

A Natureza é quântica!



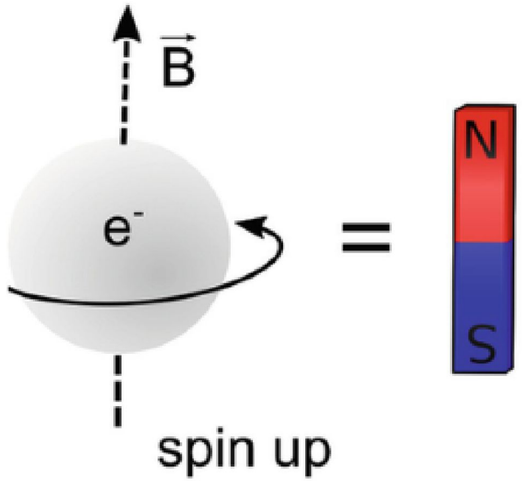
Exemplo: **SPIN de um elétron**

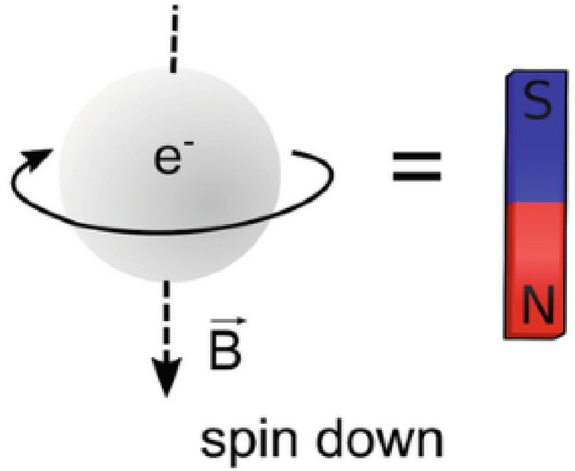


$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Representação de Dirac





|0>

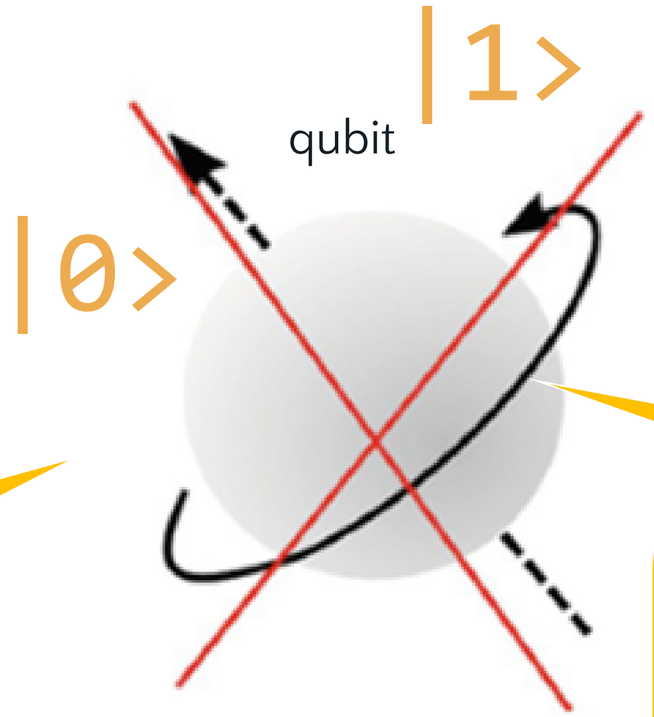
|1>

Quantum State |0 >

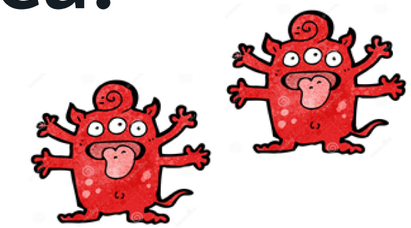
Quantum State |1 >

Em mecânica quântica, fenômenos acontecem...

Estado de Superposição



A Natureza é Quântica!

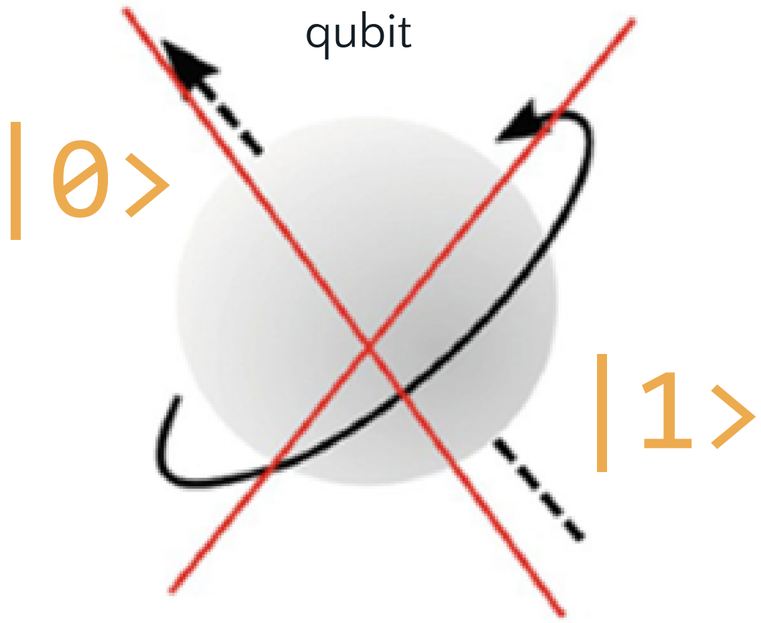


Em superposição, temos uma combinação de todos os estados ao mesmo tempo

Quando em superposição, meu qubit pode lidar com mais informações ao mesmo tempo, criando vantagem exponencial!

Como formalizar o estado de superposição!?

Superposition State



$$|\alpha|^2 + |\beta|^2 = 1$$

α e β **probabilidades** de estar em cada estado!

100% de estar em todos os estados possíveis

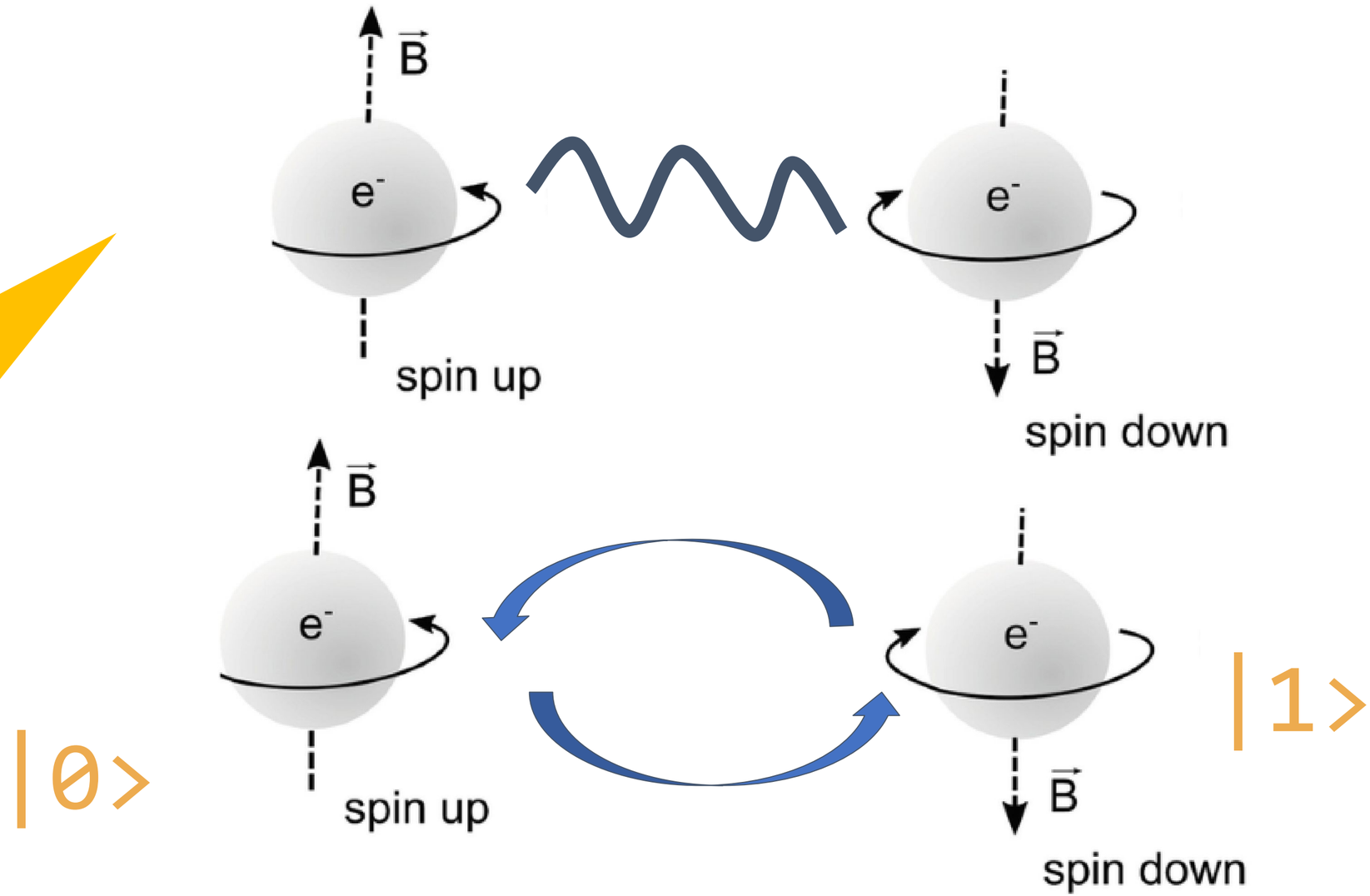
$$|\text{Qubit State}\rangle = \alpha|\text{spin up}\rangle + \beta|\text{spin down}\rangle$$

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Em mecânica quântica, fenômenos acontecem...

Estado de Emaranhamento

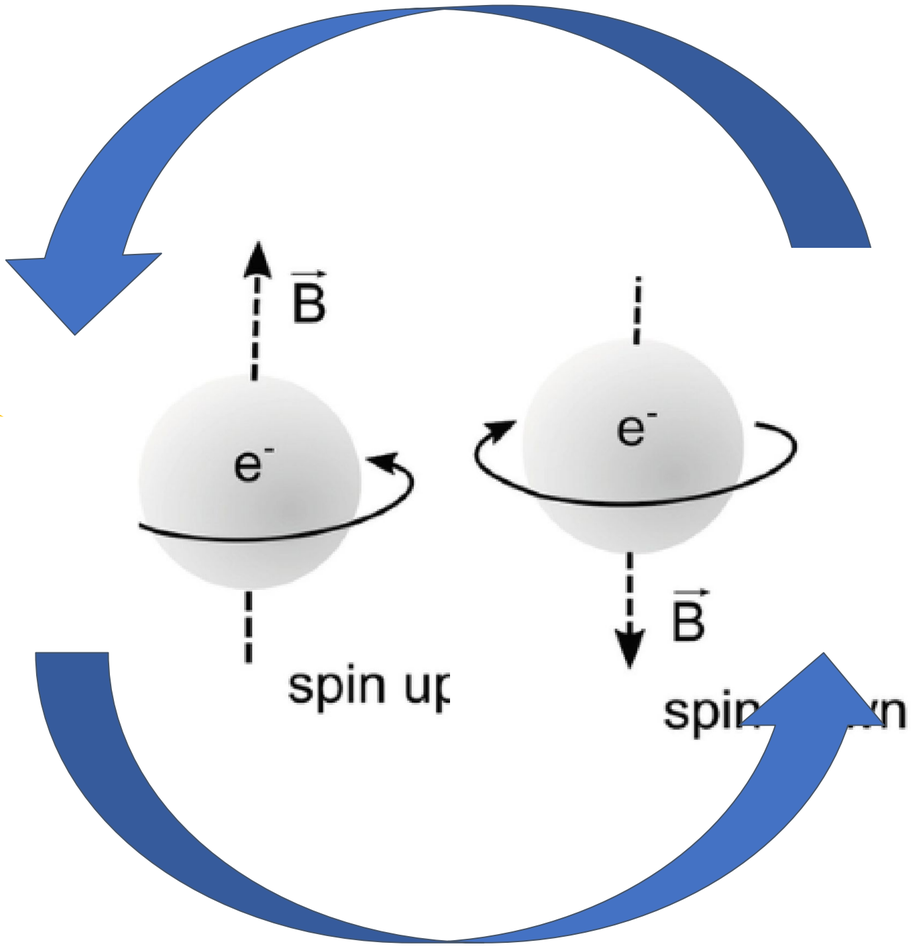
No emaranhamento, ou entrelaçamento, dois qubits interagem com polarização opostas



Em mecânica quântica, fenômenos acontecem...

Interferência

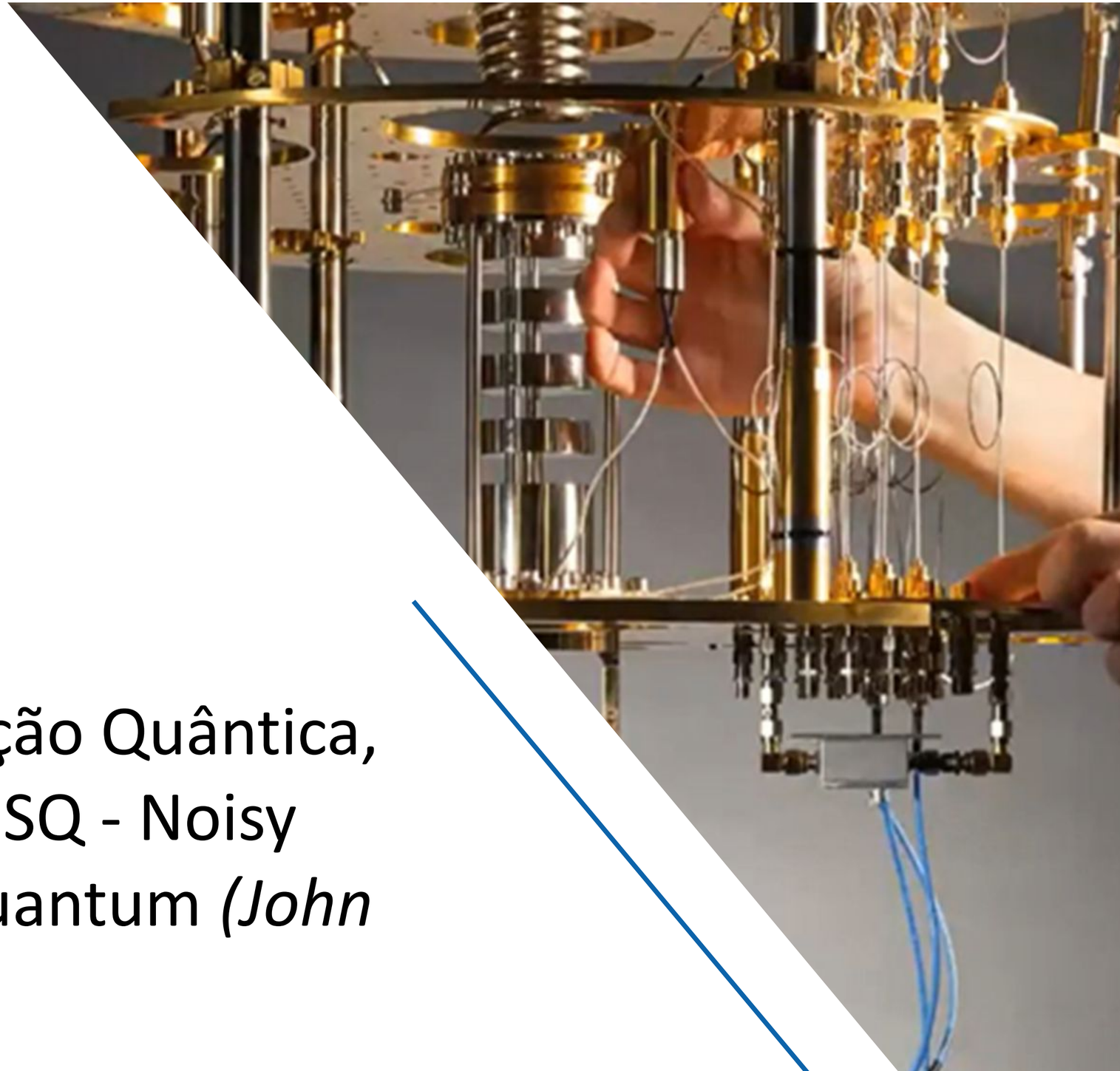
Qubits são sensíveis a Interferência, e colapsam quando ocorre algum disturbio.



Impossibilidade de cópia

A Revolução Quântica

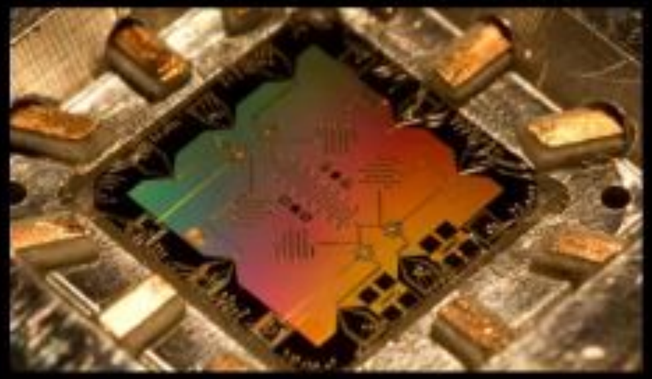
Estamos na 2º Revolução Quântica, com computadores NISQ - Noisy Intermediate-Scale Quantum *(John Preskill, 2017)*



The current options

There is no obvious winner, the market yet might split multiple ways

Superconducting



Google

rigetti IBM D-Wave

✓ Quantum supremacy
✗ Cross-talk

Trapped Ions

Honeywell

IONQ

✓ High quantum volume
✗ Slow

Photonics

ORCA Computing

XANADU

PsiQuantum

✓ Fast
✗ Many components

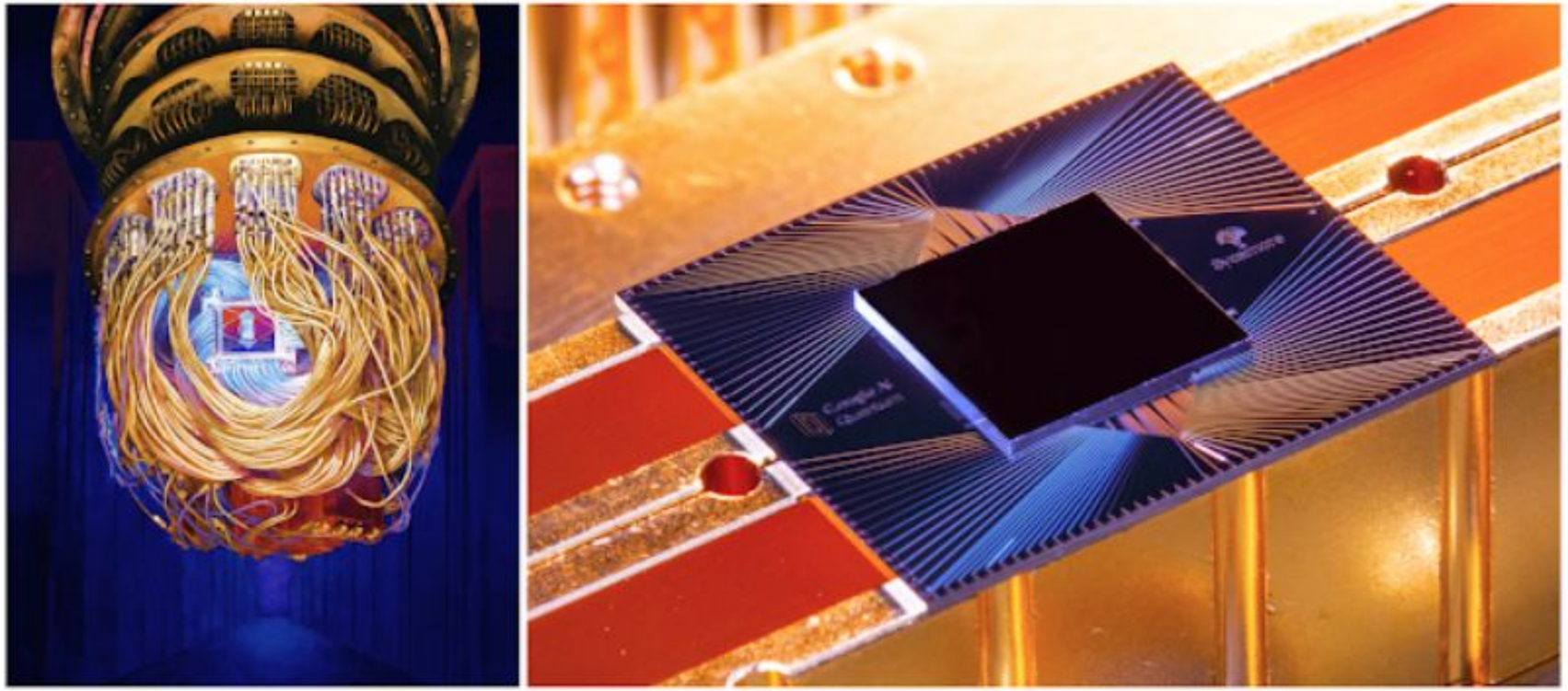
ORCA Computing, March 2022, IEEE Quantum, https://quantum.ieee.org/

Quantum Supremacy | Outubro de 2019

https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html

"We developed a new 54-qubit processor, named "Sycamore", that is comprised of fast, high-fidelity quantum logic gates, in order to perform the benchmark testing. Our machine performed the target computation in ***200 seconds,*** *and from measurements in our experiment we determined that it would take the world's fastest supercomputer* ***10,000 years*** *to produce a similar output."*

Google AI Blog

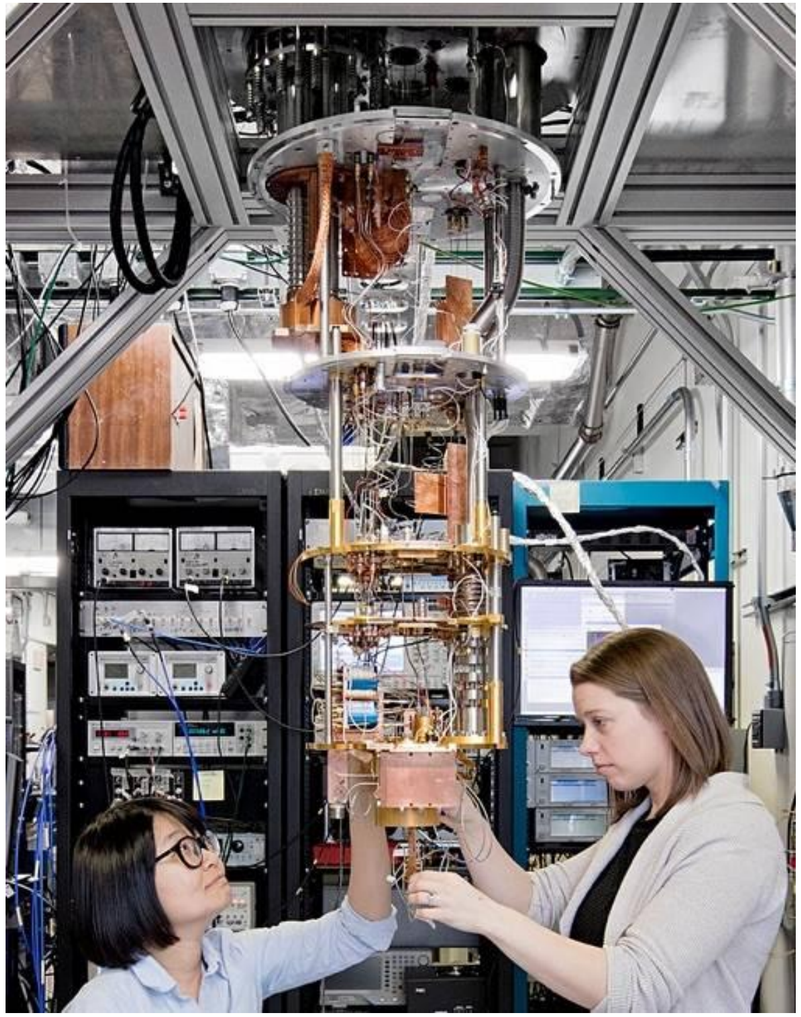


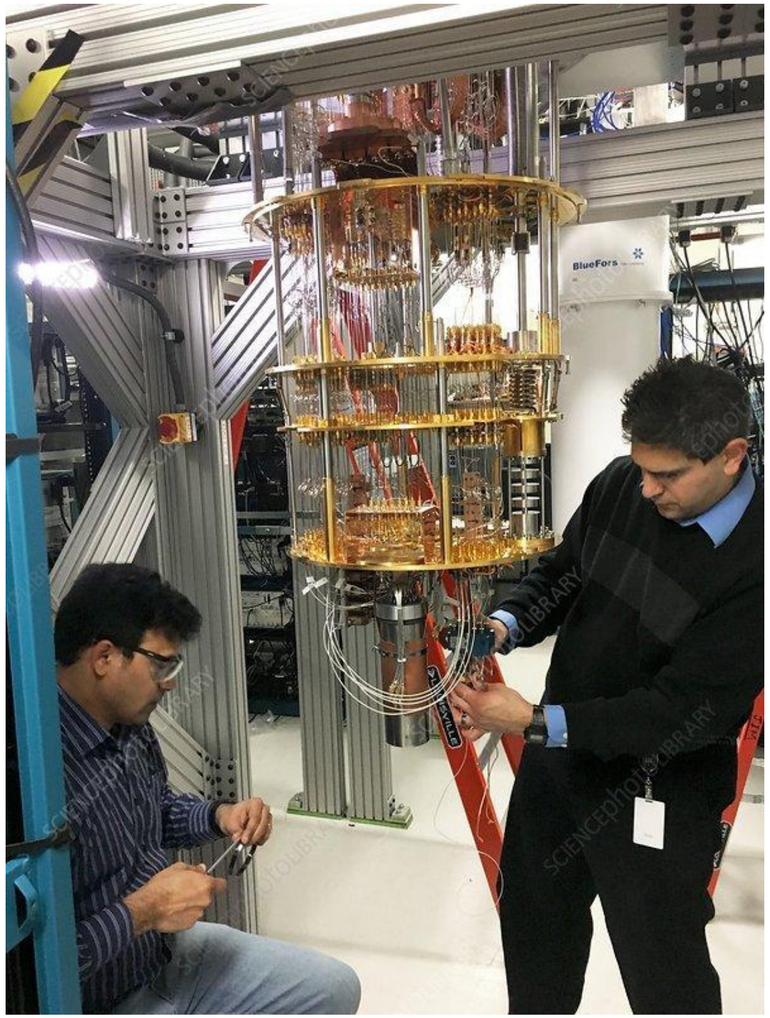
Left: Artist's rendition of the Sycamore processor mounted in the cryostat. (Full Res Version; Forest Stearns, Google AI Quantum Artist in Residence) **Right:** Photograph of the Sycamore processor. (Full Res Version; Erik Lucero, Research Scientist and Lead Production Quantum Hardware)

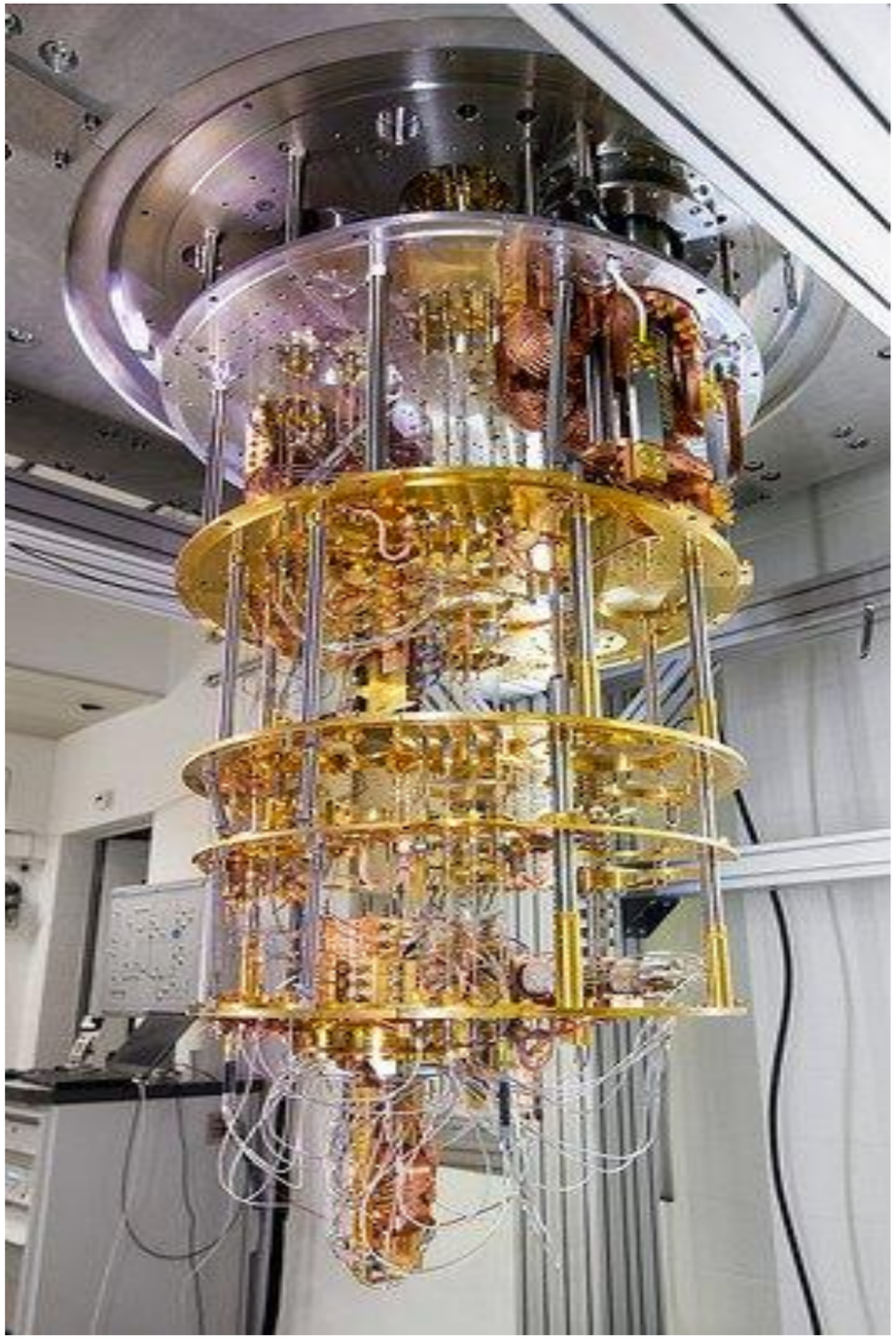
https://www.nature.com/articles/s41586-019-1666-5

IBM-QE | Superconducting

https://www.ibm.com/quantum-computing/

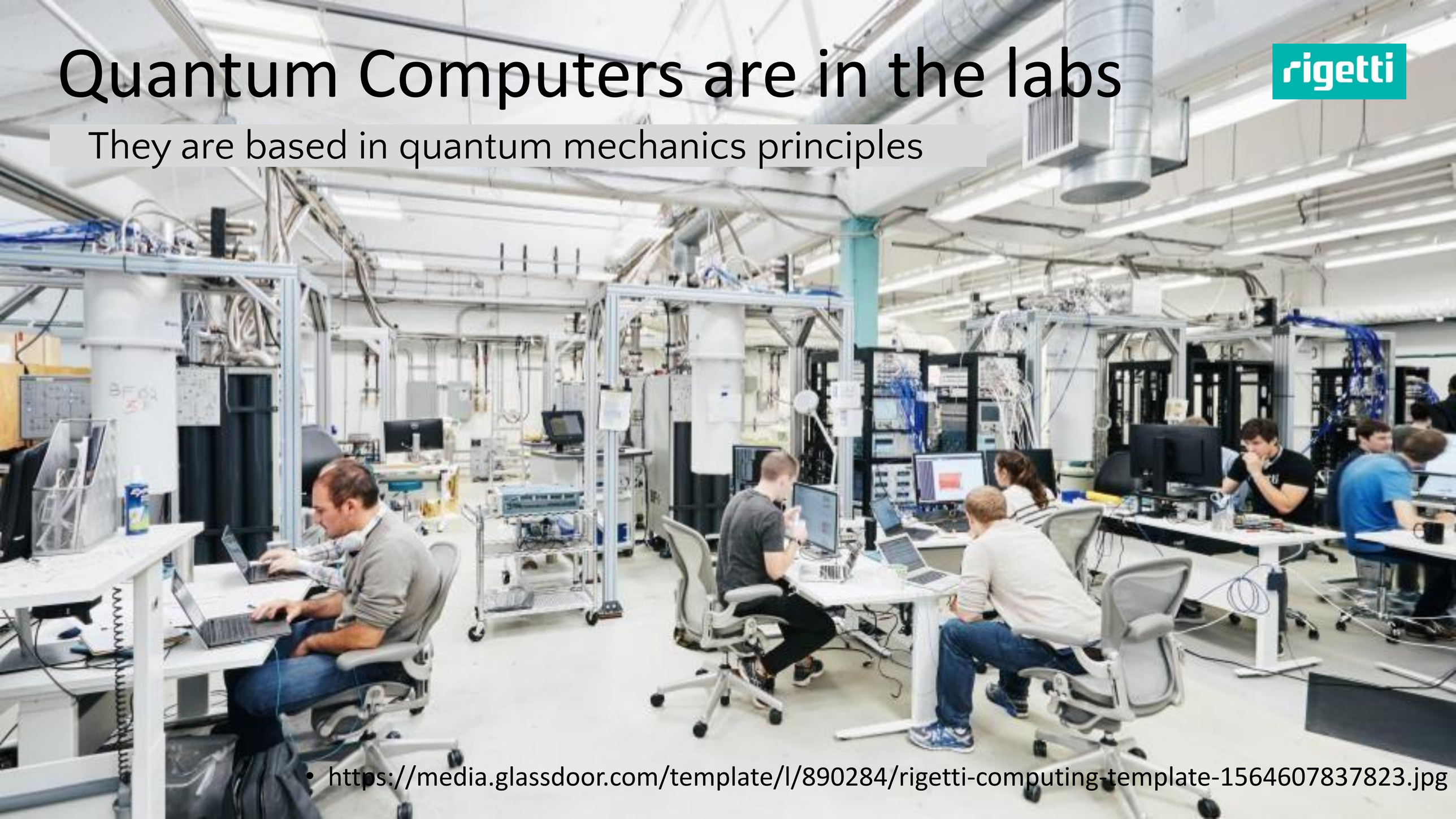






Quantum Computers are in the labs

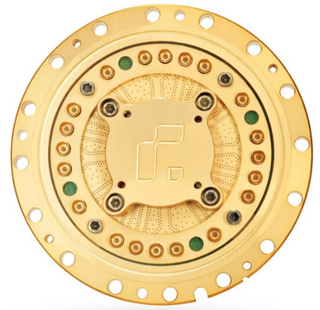
They are based in quantum mechanics principles

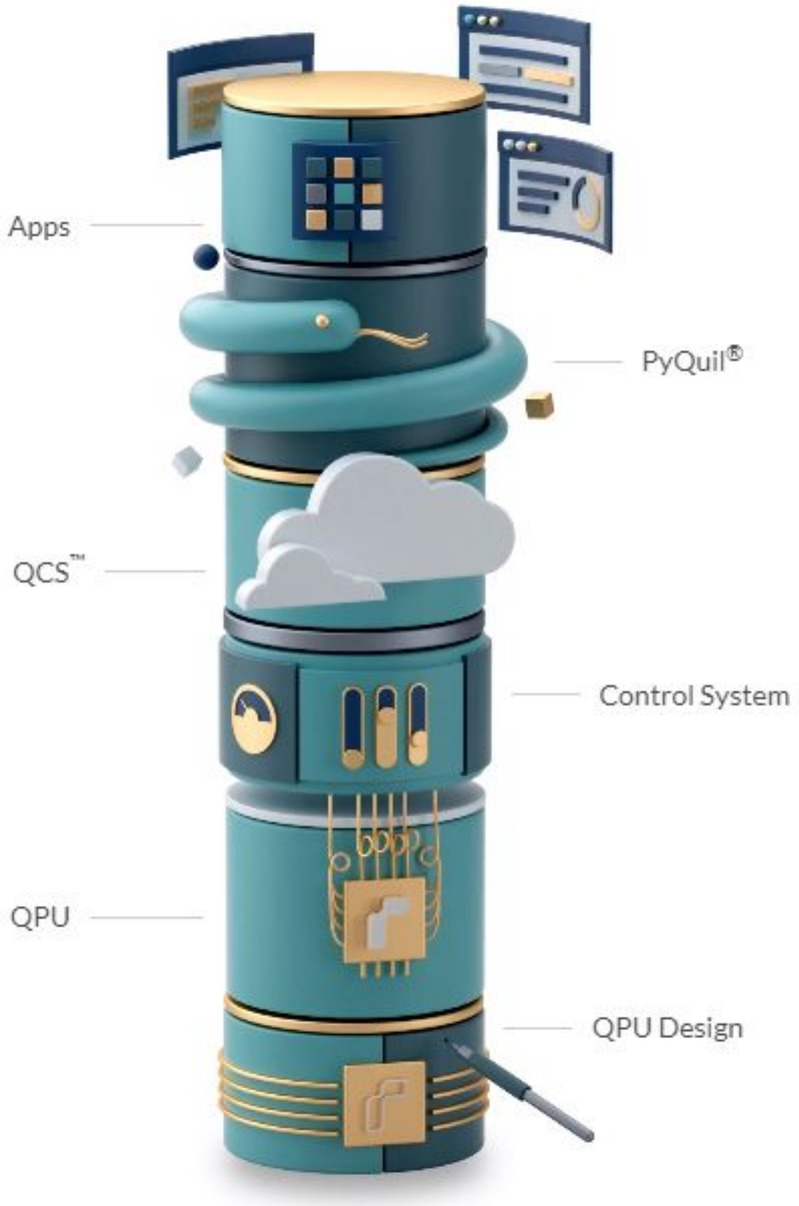


- https://media.glassdoor.com/template/l/890284/rigetti-computing-template-1564607837823.jpg

superconducting

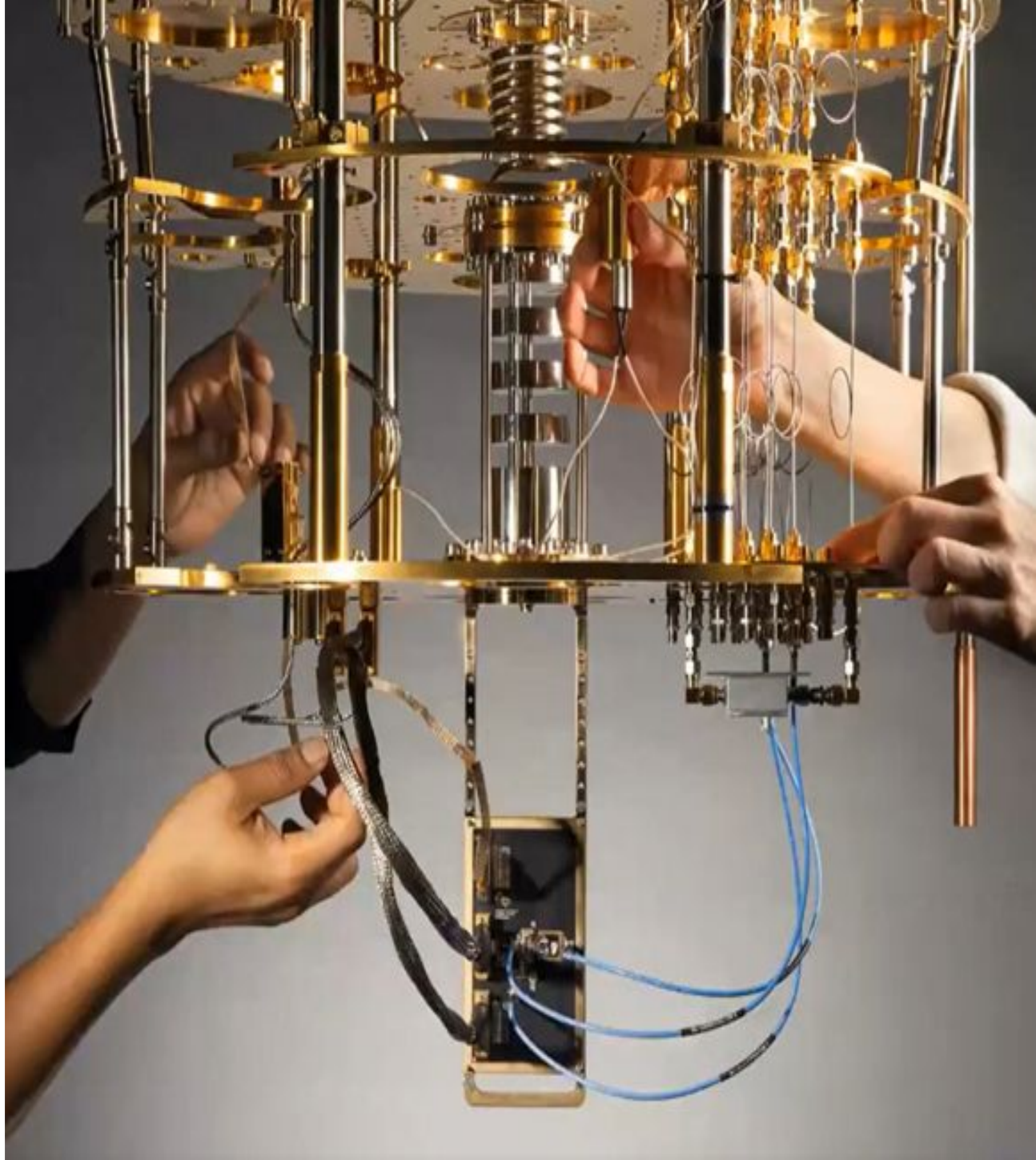
https://www.rigetti.com/





A. Nersisyan, S. Poletto, N. Alidoust, R. Manenti, et al (2019). ***"Manufacturing low dissipation superconducting quantum processors"****.* https://arxiv.org/abs/1901.08042

Criptografia Pós-Quântica ou PQCrypto



PQCrypto

Qual será o impacto da CQ nos atuais algoritmos de criptografia ?

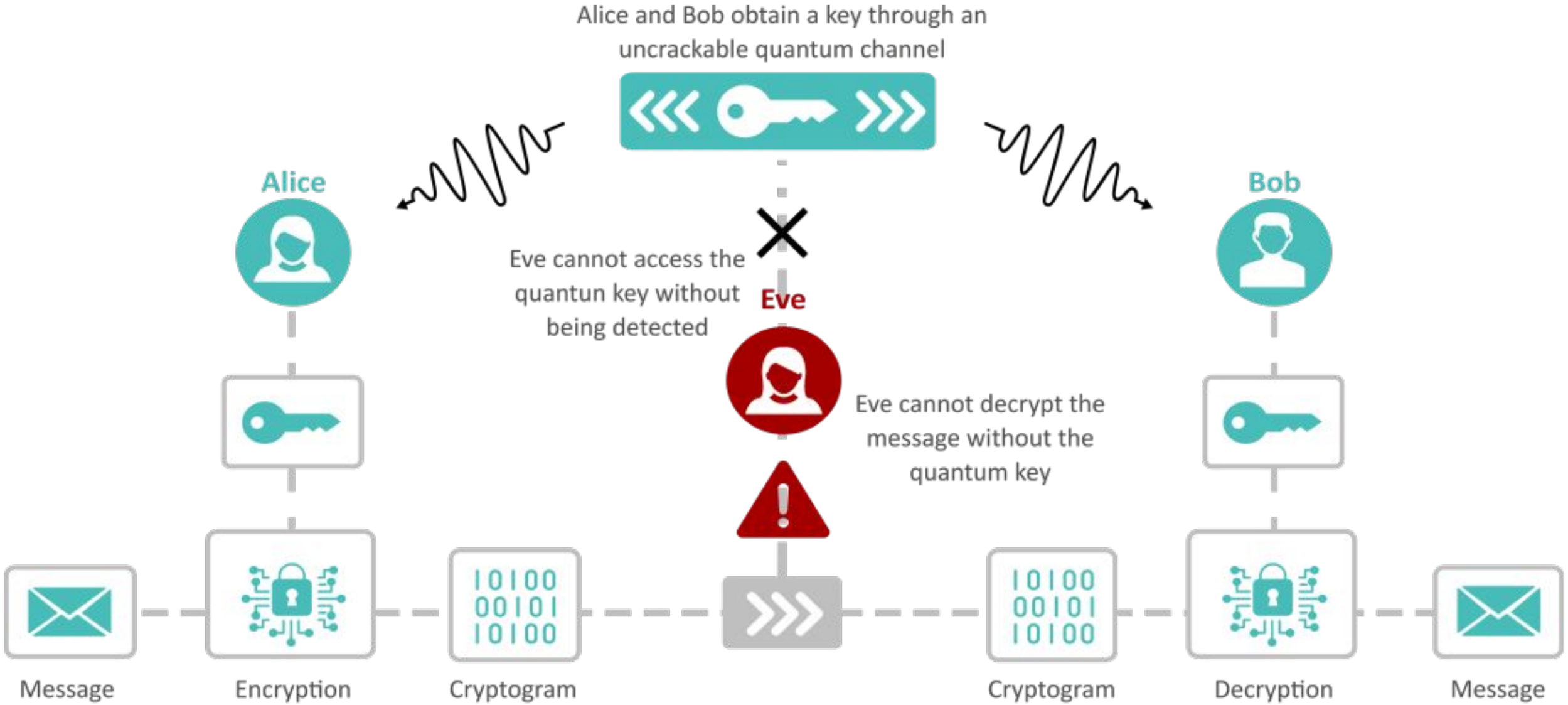
Encryption Is Everywhere – And It Will All Need to Be Replaced

Quantum Computing Will Make Current Encryption Obsolete

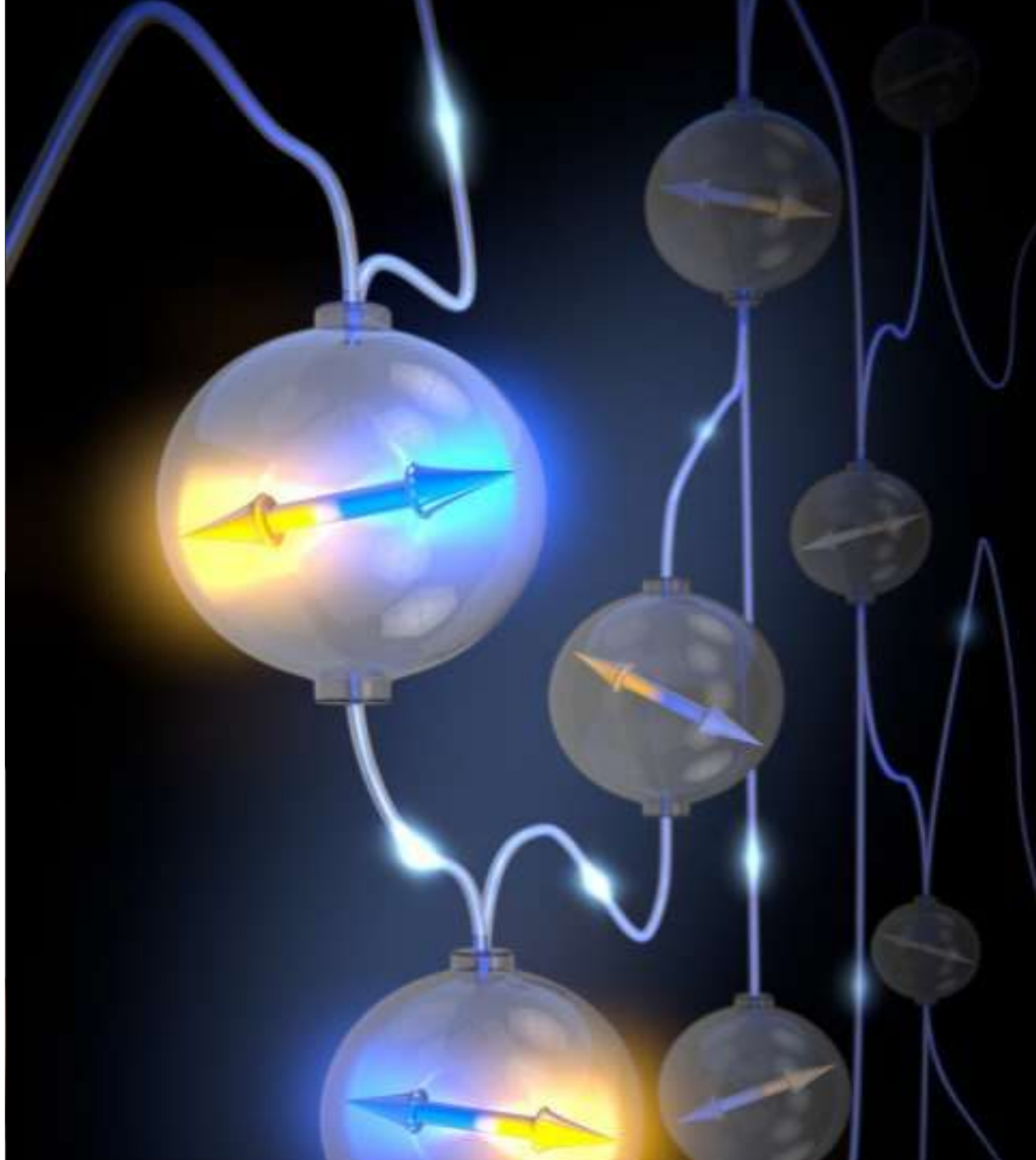
Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

https://www.venafi.com/blog/how-close-are-we-post-quantum-cryptography

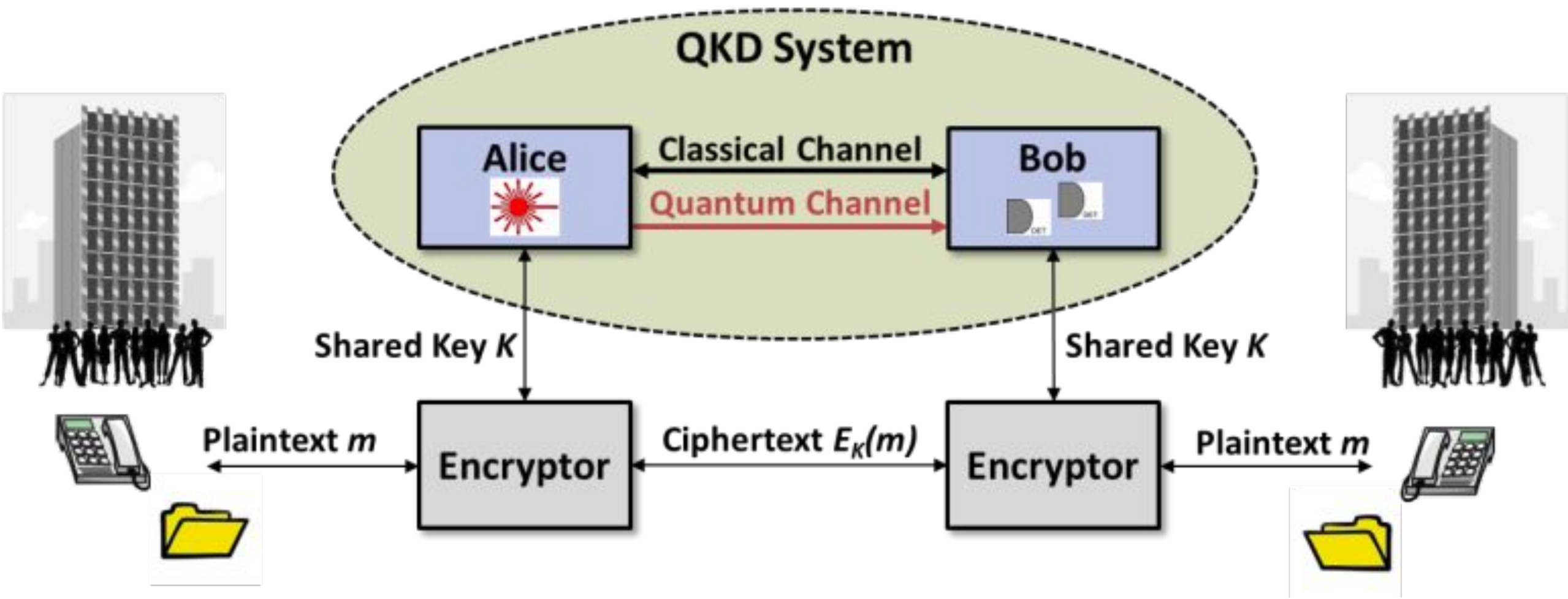
PQCrypto


Alice and Bob obtain a key through an uncrackable quantum channel
Alice
Bob
Eve cannot access the quantun key without being detected
Eve
Eve cannot decrypt the message without the quantum key
10100 00101 10100
10100 00101 10100
Message
Encryption
Cryptogram
Cryptogram
Decryption
Message
Alice encrypts a message for Bob
Bob receives and decrypts message

Comunicação Quântica

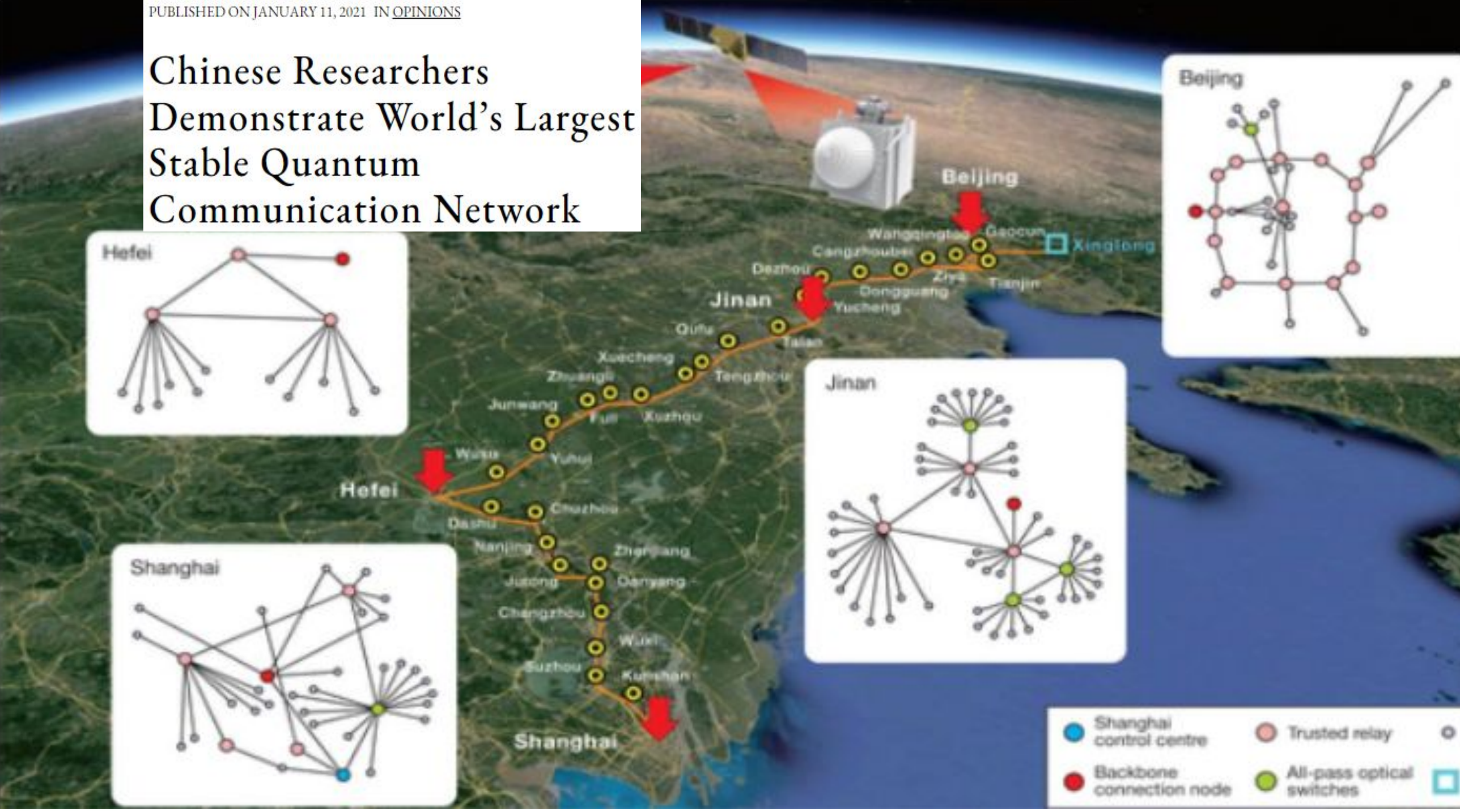


QKD - Quantum Key Distribution



PUBLISHED ON JANUARY 11, 2021 IN OPINIONS

Chinese Researchers Demonstrate World's Largest Stable Quantum Communication Network



SwissQuantum QKD

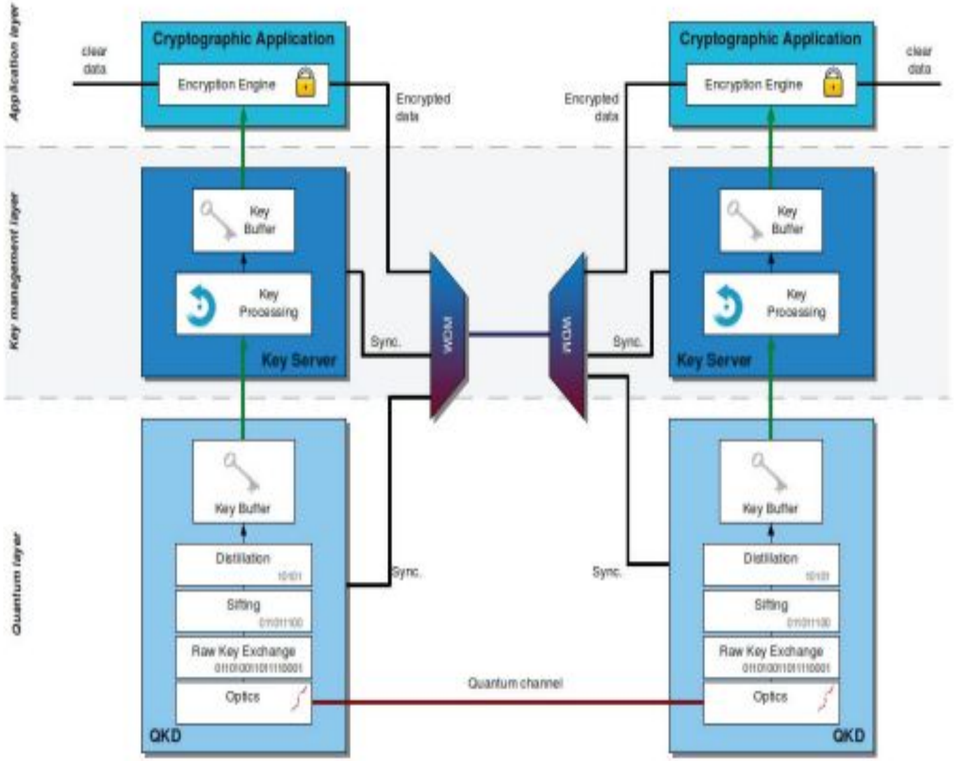
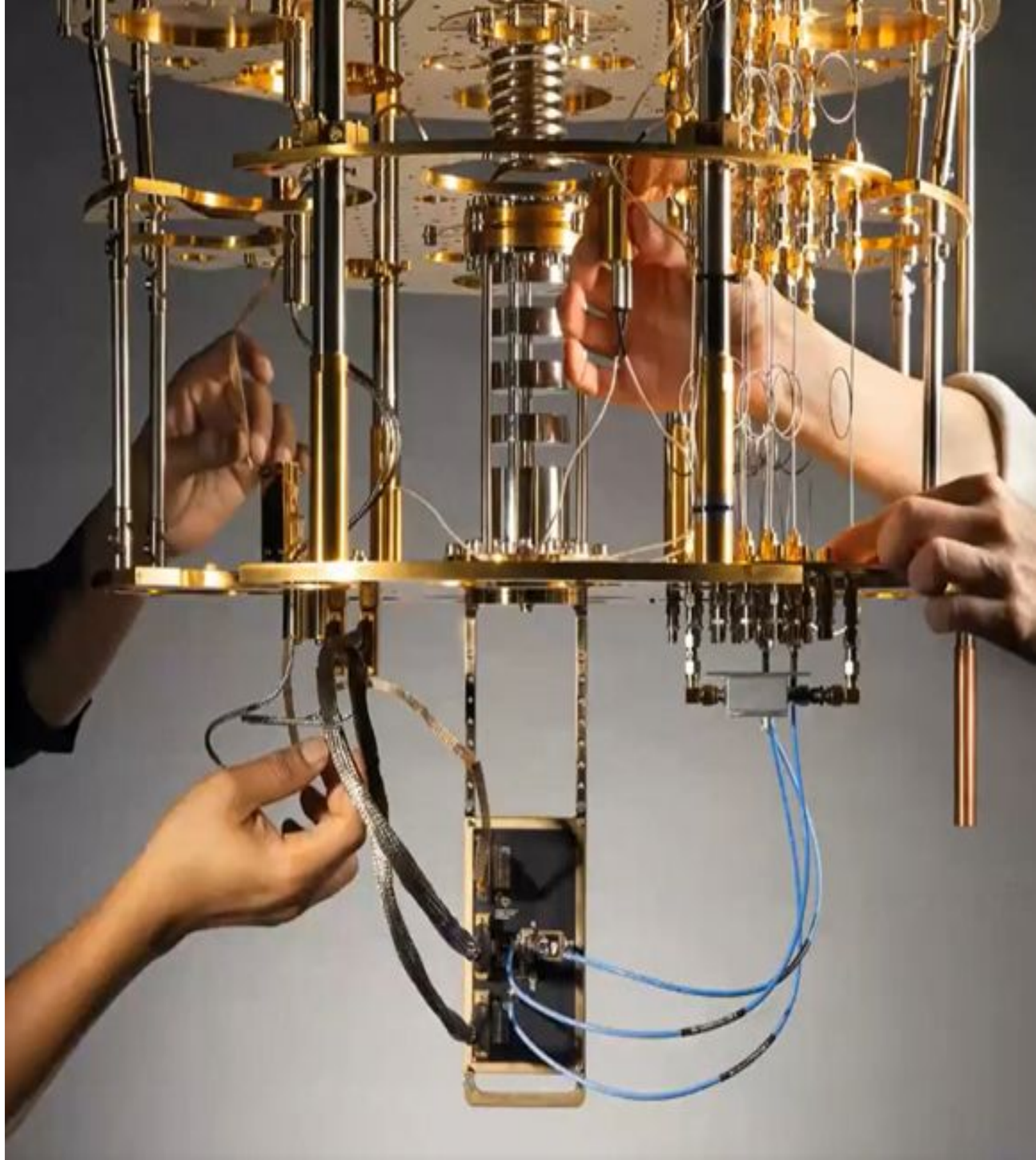


Figure 1. Map of the SwissQuantum network. Two nodes are in the Geneva city centre and the third one is on the site of CERN in France (the border is in red). The white lines are drawn for illustration: they do not represent the fibres.

Stucki, D., Legre, M., Buntschu, F., Clausen, B., Felber, N., Gisin, N., ... & Zbinden, H. (2011). Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New Journal of Physics*, *13*(12), 123001.

O que podemos fazer com CQ atualmente?



Potential applications of quantum computing | 2019

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

- **Machine learning:** Improved ML through faster stru rediction. Examples include Boltzmann machines, quantum Bolt semisupervised learning, unsupervised learning an
- **Artificial intelligence** on, comprehensi ers.
- **C** hemistries will all drive improvements gs, tailored drugs, and maybe even hair restorer.
- uantum computing could enable faster, more complex Monte Carlo mulations; for example, trading, trajectory optimization, market instability, price optimization and hedging strategies.
- **Healthcare:** DNA gene sequencing, such as radiotherapy treatment optimization/brain tumor detection, could be performed in seconds instead of hours or weeks.
- **Materials:** super strong materials; corrosion proof paints; lubricants; semiconductors
- **Computer science:** Faster multidimensional search functions; for example, query optimization, mathematics and simulations.

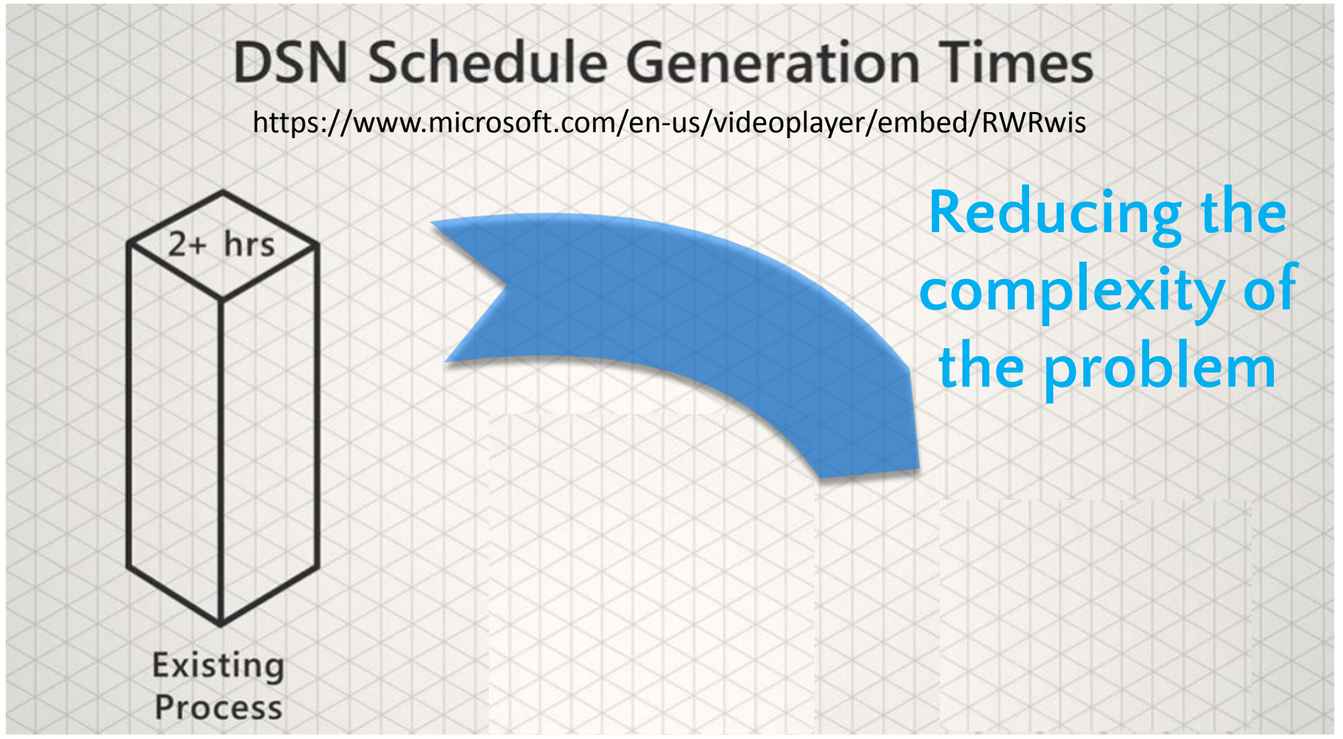
"By 2023, 20% of organizations will be budgeting for quantum computing projects"

Microsoft+NASA | Quantum Optimization | Feb 2022

https://www.geekwire.com/2022/nasas-jet-propulsion-lab-uses-microsofts-azure-quantum-to-ease-deep-space-networks-traffic-jam/

NASA's Jet Propulsion Lab uses Microsoft's Azure Quantum to ease Deep Space Network's traffic jam

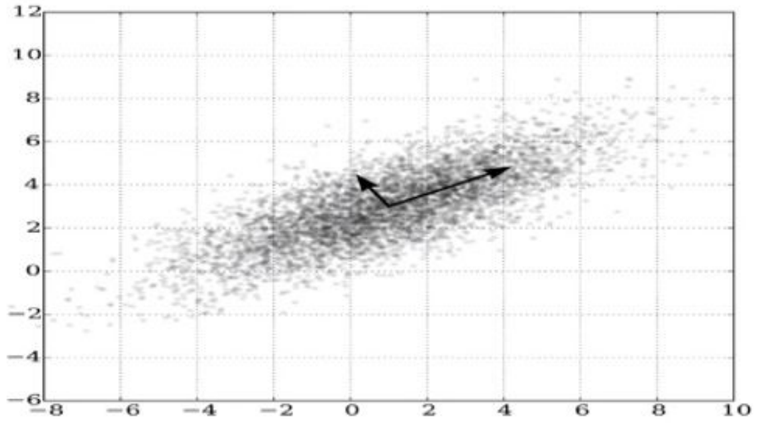
BY ALAN BOYLE on January 27, 2022 at 9:00 am



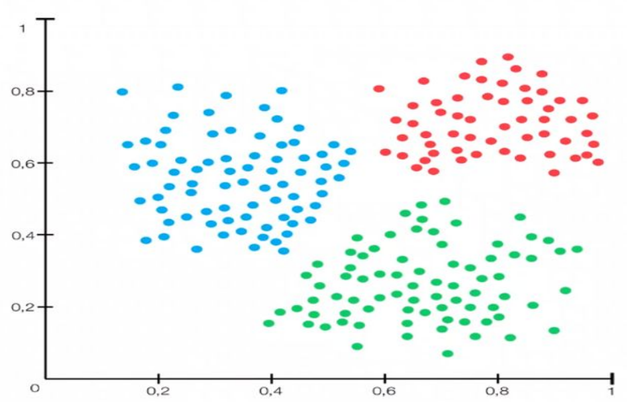
Quantum Computing para Finanças

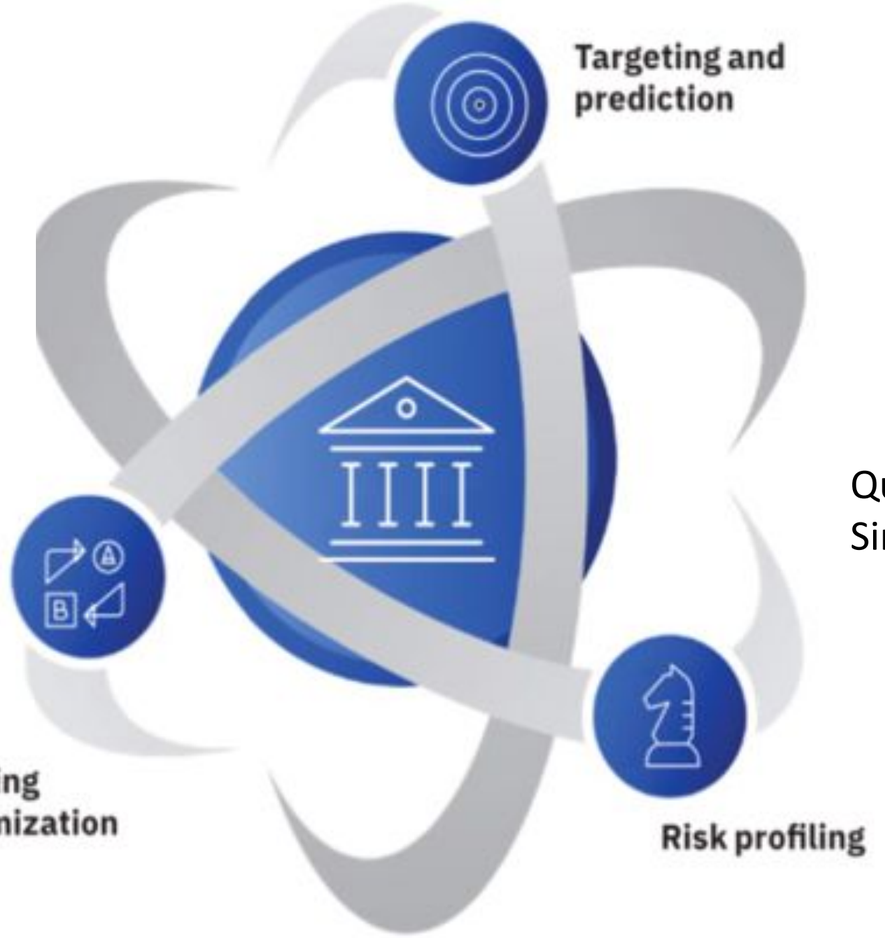
Quantum Machine Learning e Quantum Simulation

Quantum Speedup in Principle Component Analysis (PCA)

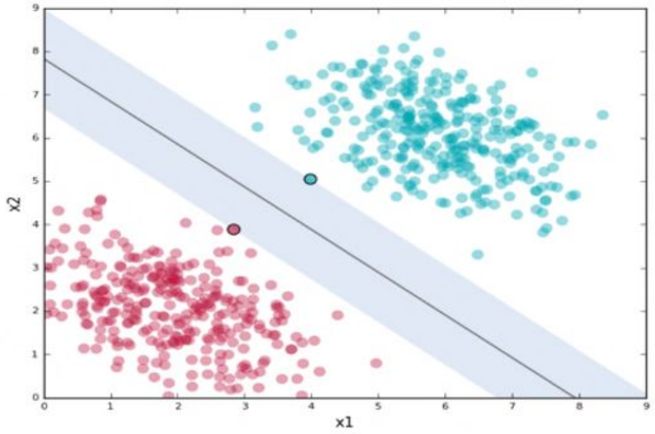


Quantum Speedup in Clustering

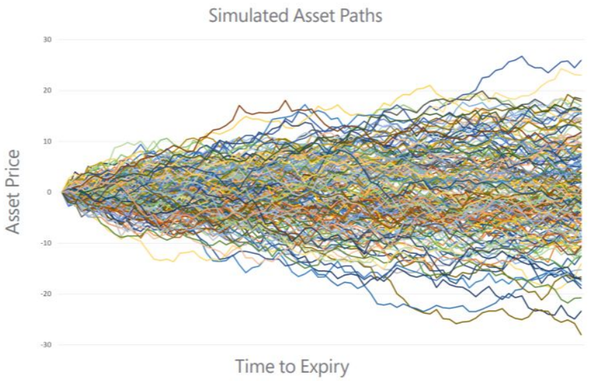




Quantum Speedup in Support Vector Machine (SVM)



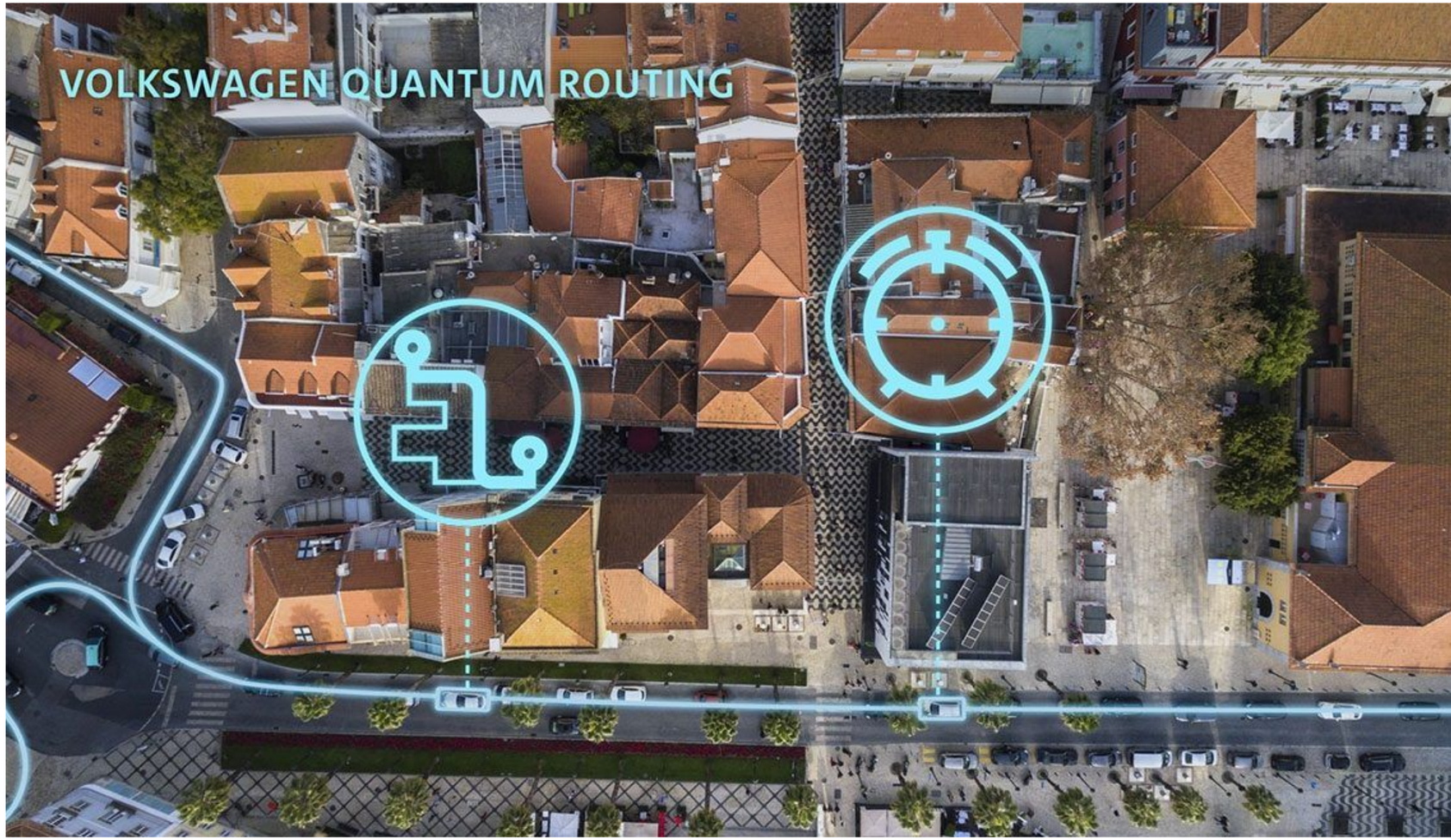
Quantum Speedup for Monte Carlo Simulations



Volkswagen utiliza CQ para otimização

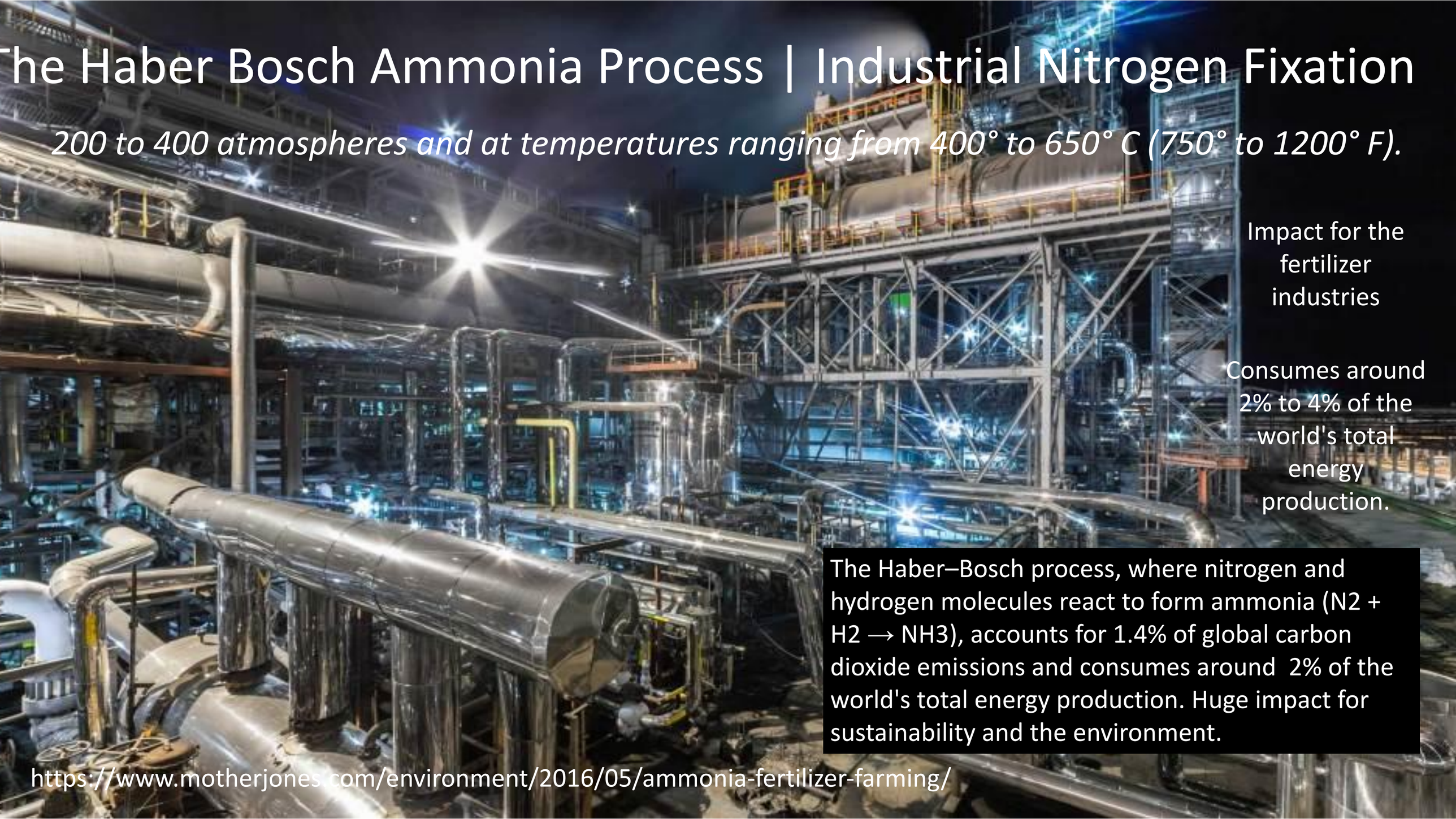
O uso de CQ está presente em alguns projetos internos da VW:

- Para calcular rotas que evite congestionamentos
- Para melhorar o desempenho de baterias de carros elétricos



The Haber Bosch Ammonia Process | Industrial Nitrogen Fixation

200 to 400 atmospheres and at temperatures ranging from 400° to 650° C (750° to 1200° F).



Impact for the fertilizer industries

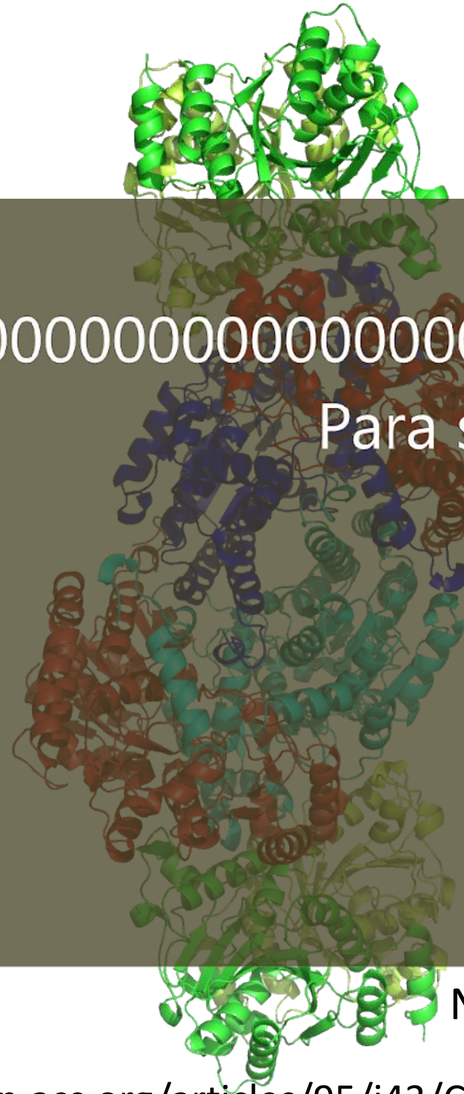
Consumes around 2% to 4% of the world's total energy production.

The Haber–Bosch process, where nitrogen and hydrogen molecules react to form ammonia ($N_2 + H_2 \rightarrow NH_3$), accounts for 1.4% of global carbon dioxide emissions and consumes around 2% of the world's total energy production. Huge impact for sustainability and the environment.

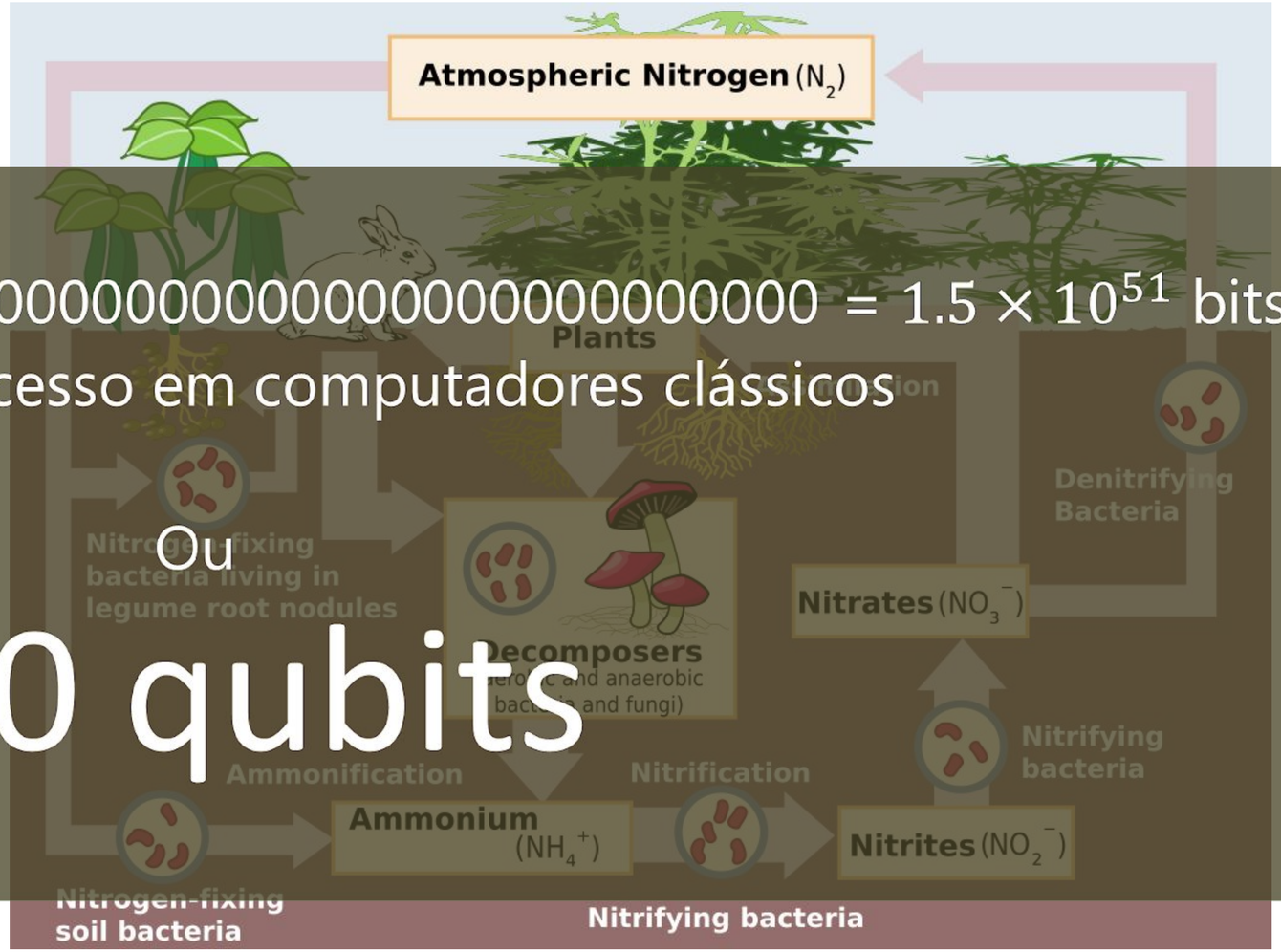
https://www.motherjones.com/environment/2016/05/ammonia-fertilizer-farming/

Fixação de Nitrogênio em temperature ambiente

Biological nitrogen fixation (BNF) | Chemistry is quantum´s killer app (2017)



Nitrogenase



$150000000000000000000000000000000000000000000000 = 1.5 \times 10^{51}$ bits

Para simular o processo em computadores clássicos

Ou

170 qubits

https://cen.acs.org/articles/95/i43/Chemistry-quantum-computings-killer-app.htm

100-200
qubits

Fixação de Nitrogênio

Impacto para a indústria de fertilizantes

Revisão de inúmeros processos da indústria química

100-200
qubits

Captura de Carbono

Mitigação para o aquecimento global

Simulações meteorológicas

Saúde Planetária

Soluções de sustentabilidade

Estudos sobre mudanças climáticas

100-1000
qubits

Novos Materiais

Criação de novas baterias

Novos Produtos

Impacto para a indústria de fármacos

100-1000
qubits

Artificial Intelligence

Aprendizado de máquina quântico

Inteligência Artificial quântica

Redução do tempo de treinamento em Machine Learning

HOW DOES QUANTUM IMPACT HEALTHCARE?

Quantum sensors

- Locating surgical tools
- Locating tumors & checking full removal

Quantum sensors

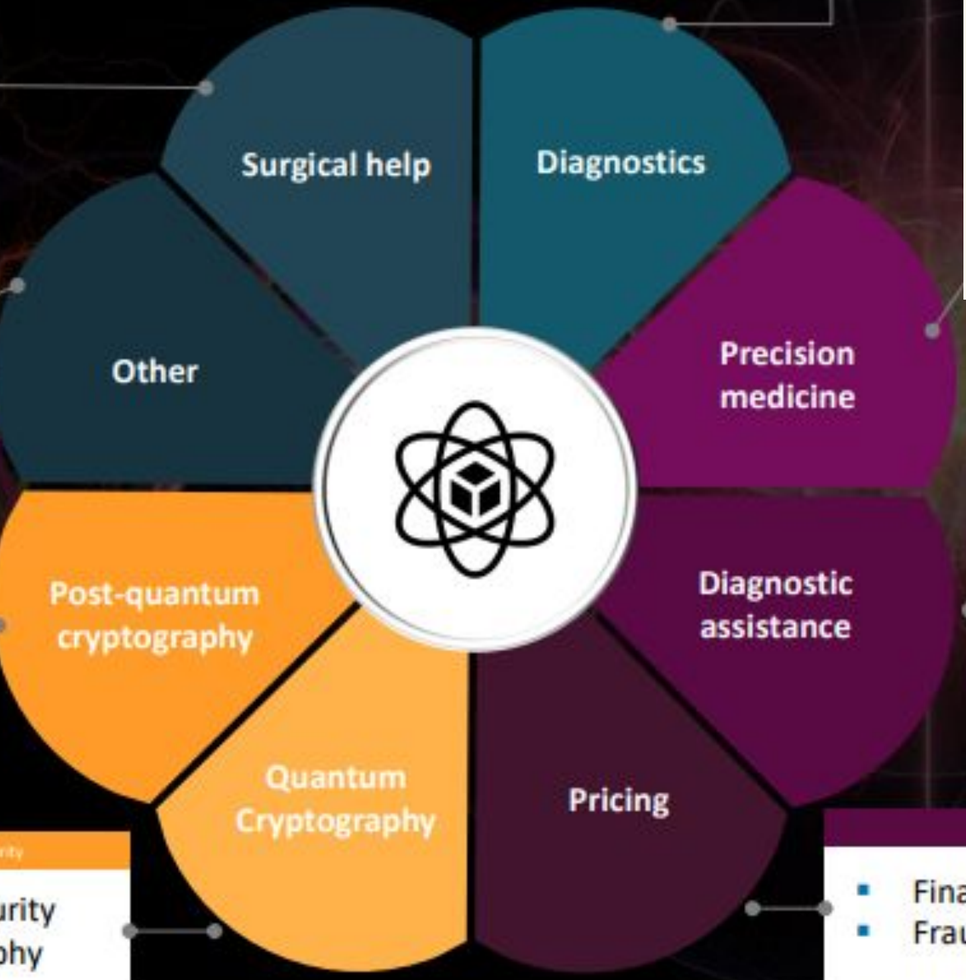
- Drug delivery
- Personal Healthcare

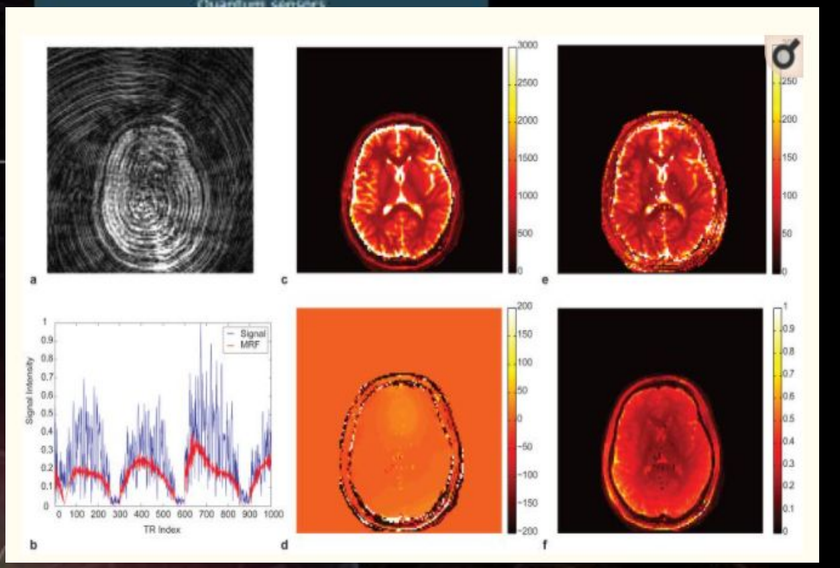
Networking & Security

- Confidential computing
- Data sharing
- Data storage

Networking & Security

- Cyber Security
- Cryptography





Quantum Computing

- Analysis of medical images
- Classification of biochemical characteristics
- flow cytometry and single-cell sequencing

Quantum Computing

- Financial risk analysis
- Fraud detection

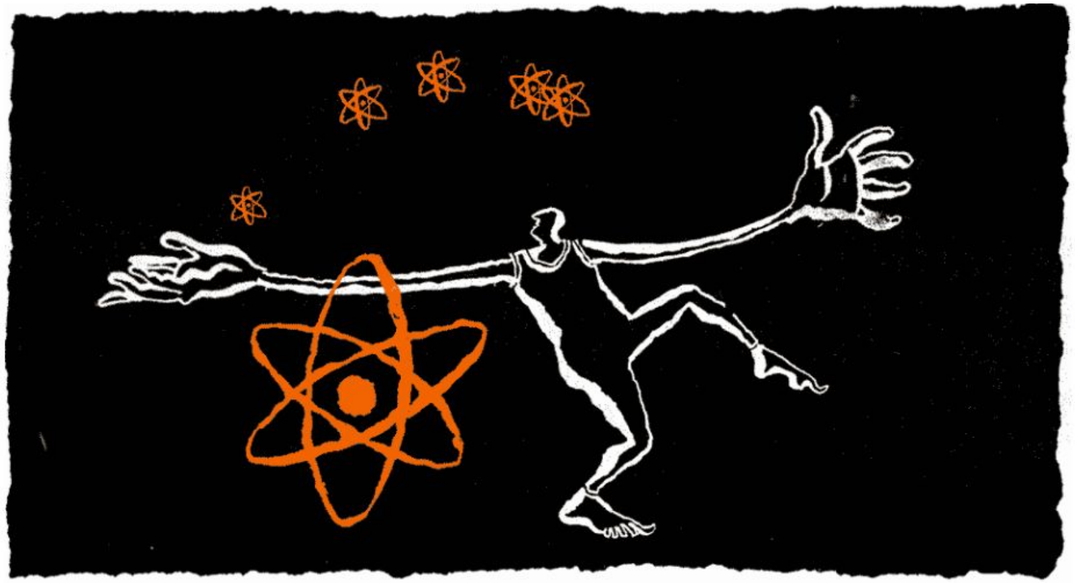
IEEE Quantum Computing Healthcare Summit - IEEE Quantum, Feb 2022

Investimentos em tecnologias quânticas

Grande interesse nos últimos 5 - 10 anos.

Quantum Computing @ The Economist | 2017

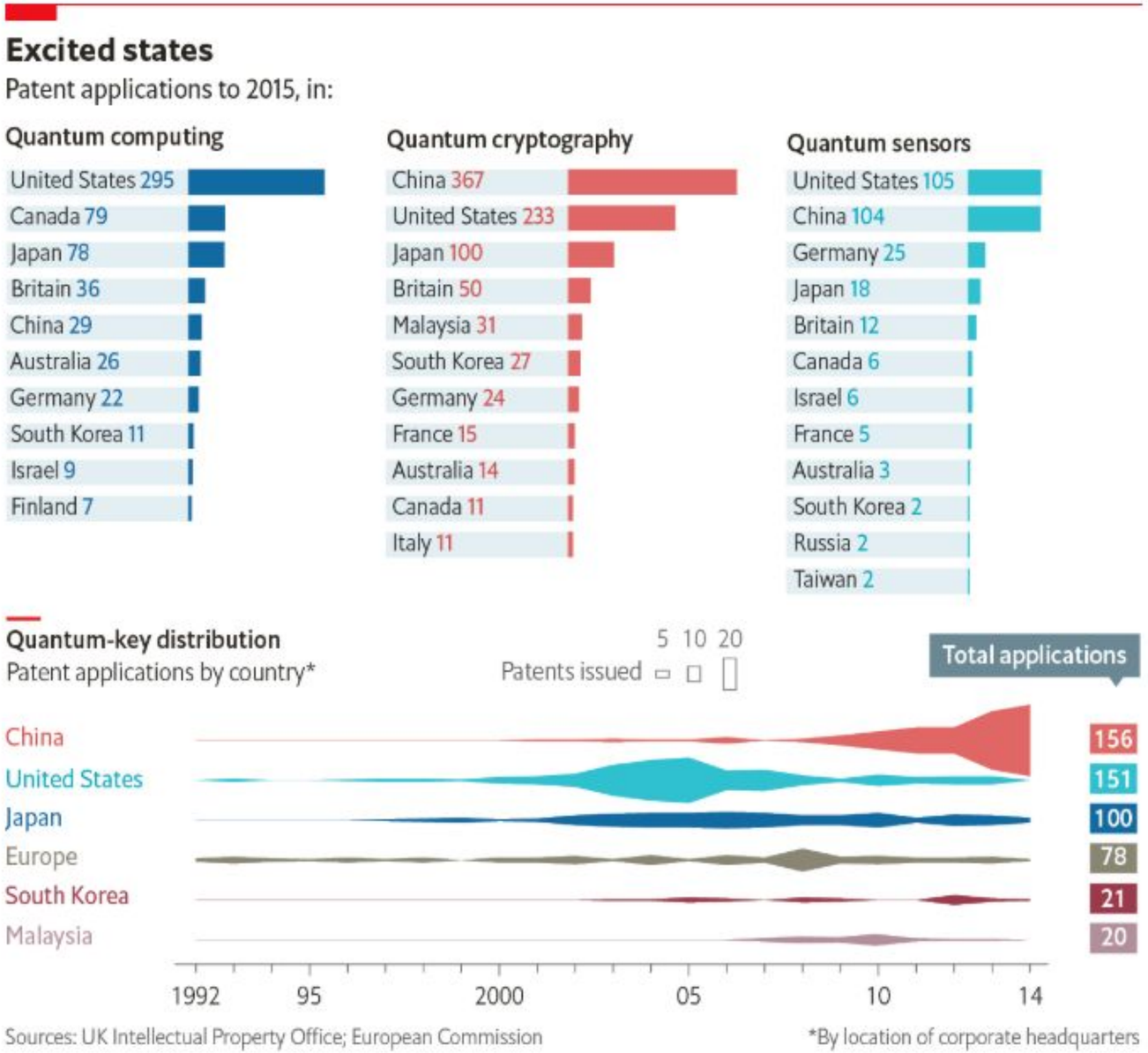
https://www.economist.com/news/essays/21717782-quantum-technology-beginning-come-its-own



TECHNOLOGY QUARTERLY | 2017

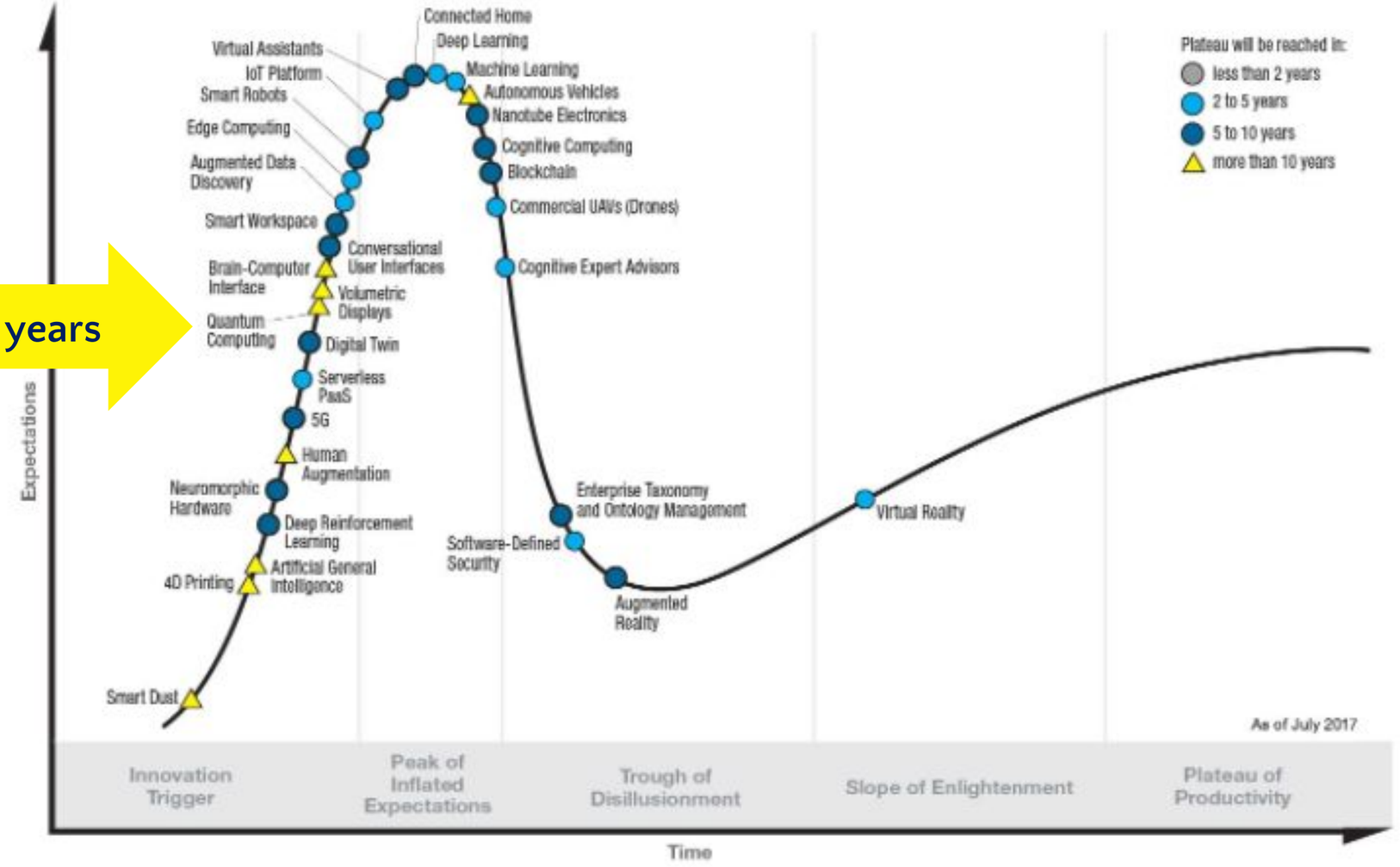
Quantum technology is beginning to come into its own

The Economist



Gartner Hype Cycle for Emerging Technologies, 2017

more than 10 years



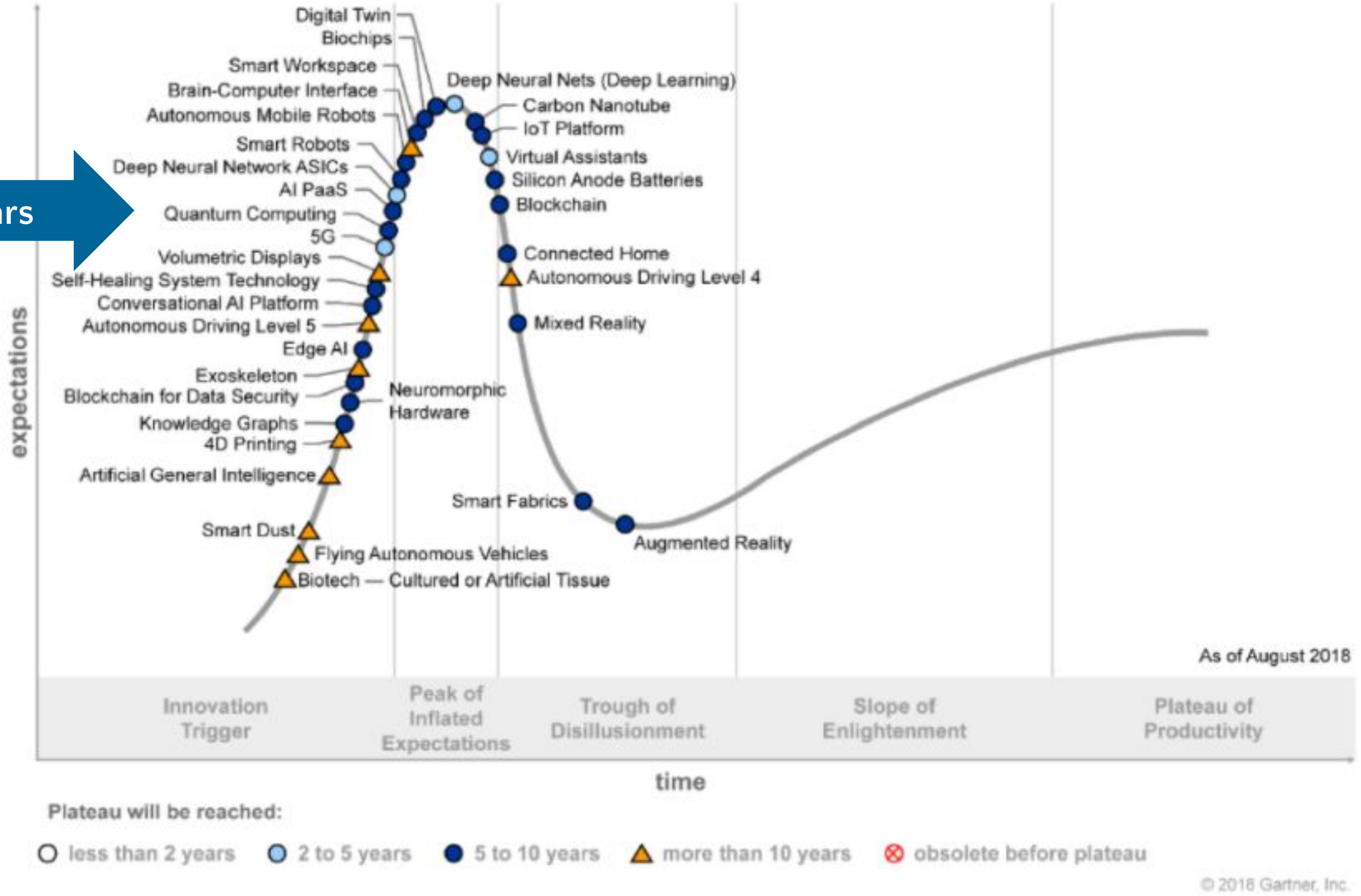
gartner.com/SmarterWithGartner

Gartner

Figure 1. Hype Cycle for Emerging Technologies, 2018

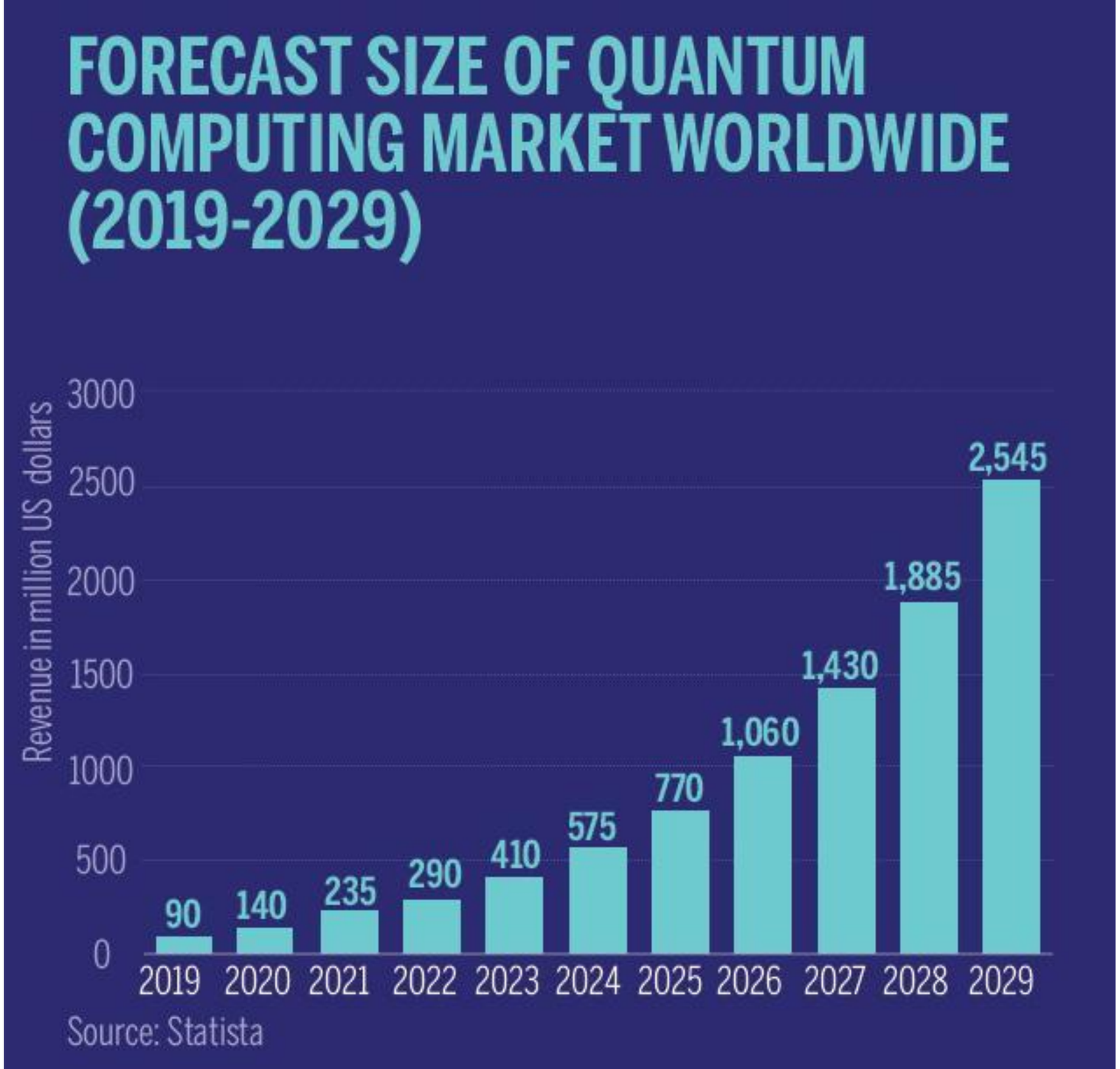
2018 | Gartner

5 to 10 years

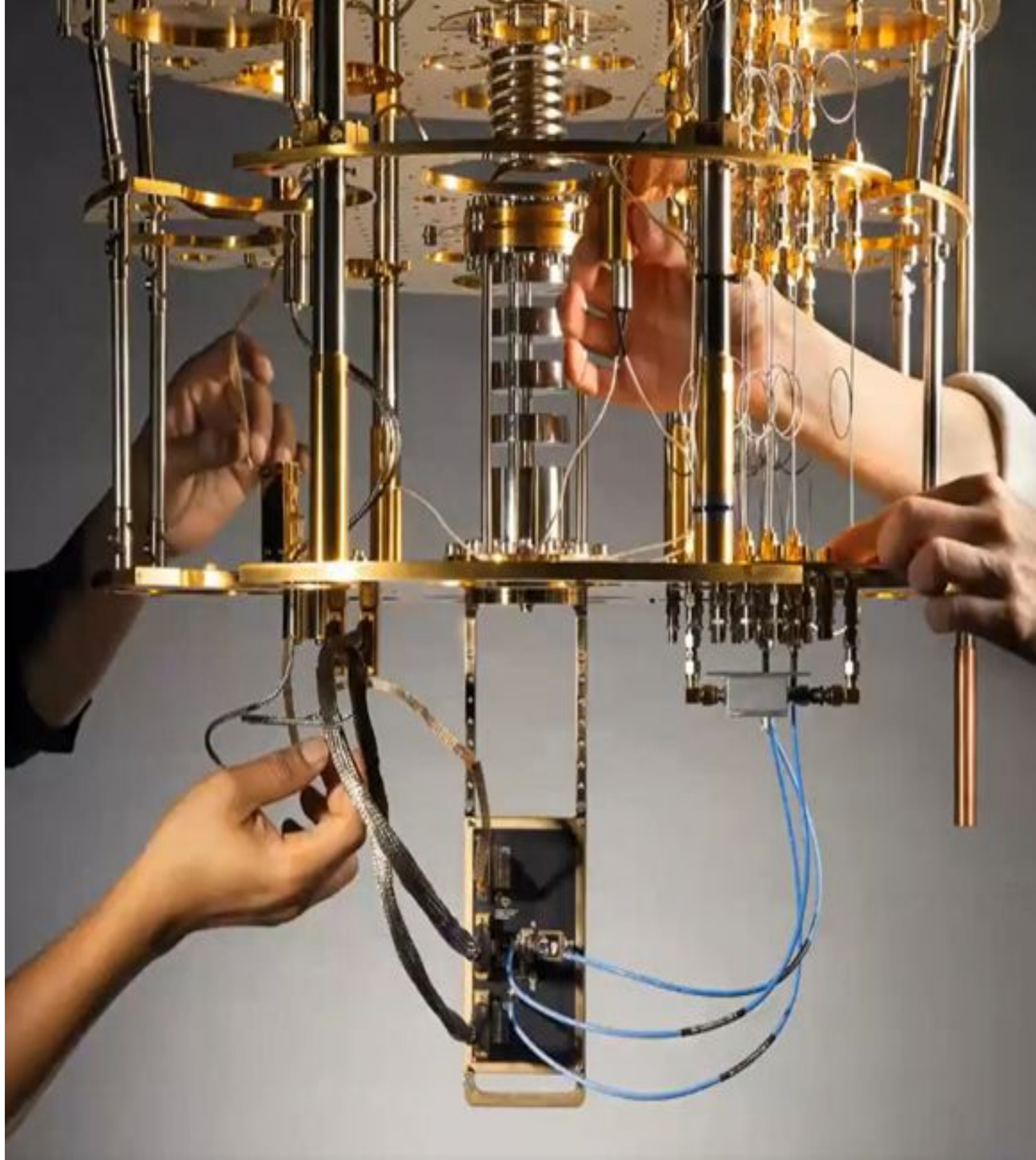


https://www.gartner.com/en/newsroom/press-releases/2018-08-20-gartner-identifies-five-emerging-technology-trends-that-will-blur-the-lines-between-human-and-machine

Expectativa de investimento em QC

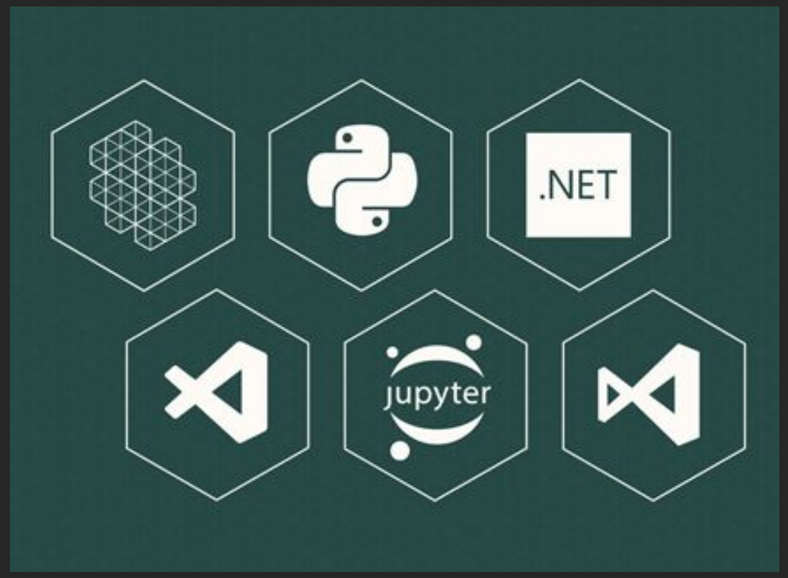


Simuladores e Ferramentas para Programação Quântica



https://github.com/microsoft/quantum

Quantum Development Kit



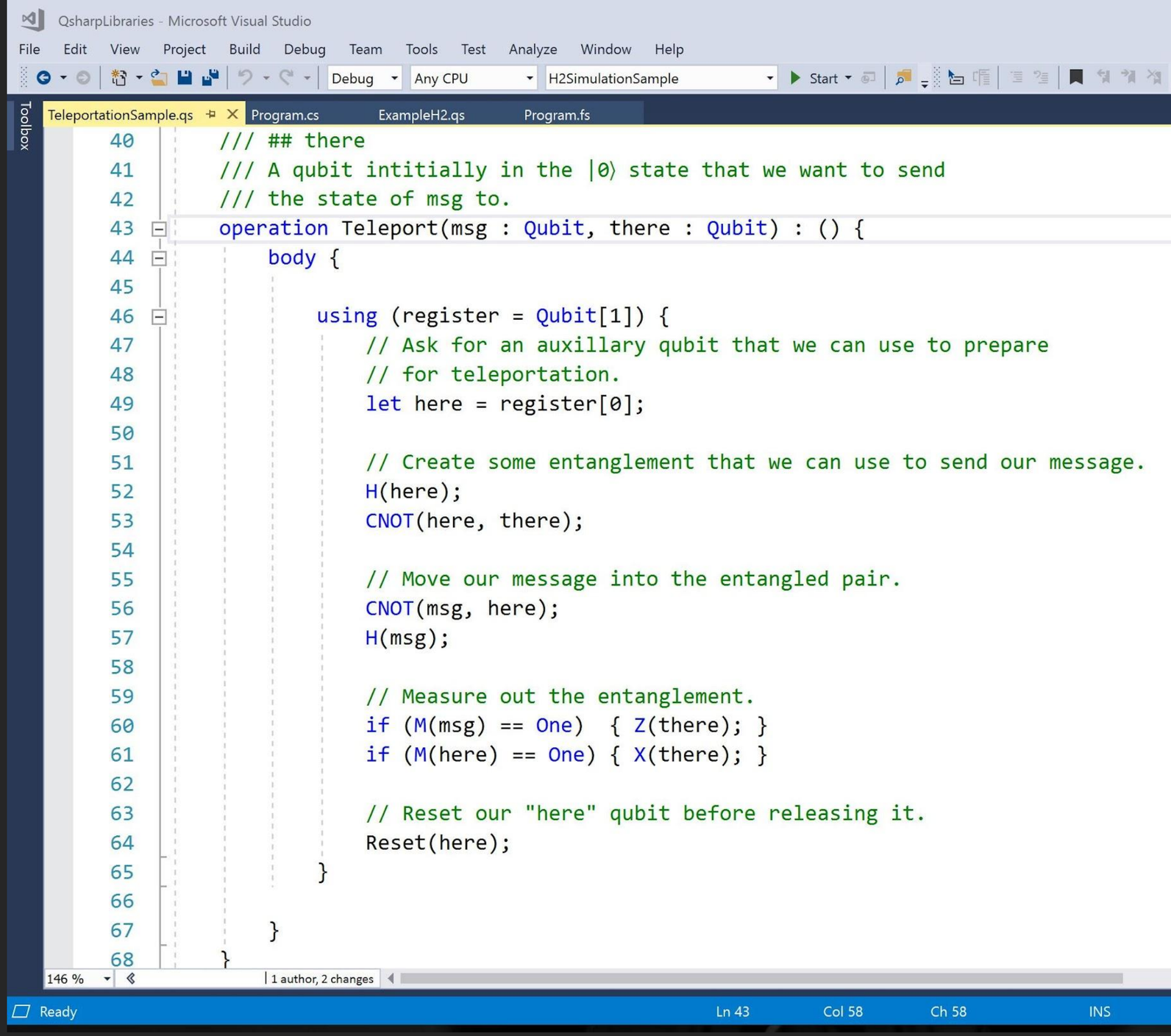
Quantum-focused programming language

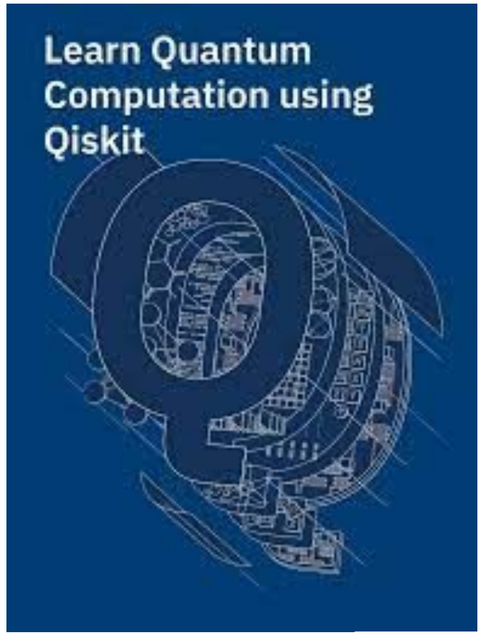
Local & Azure simulators

Sample code & libraries

Quantum-focused programming language (Q#)

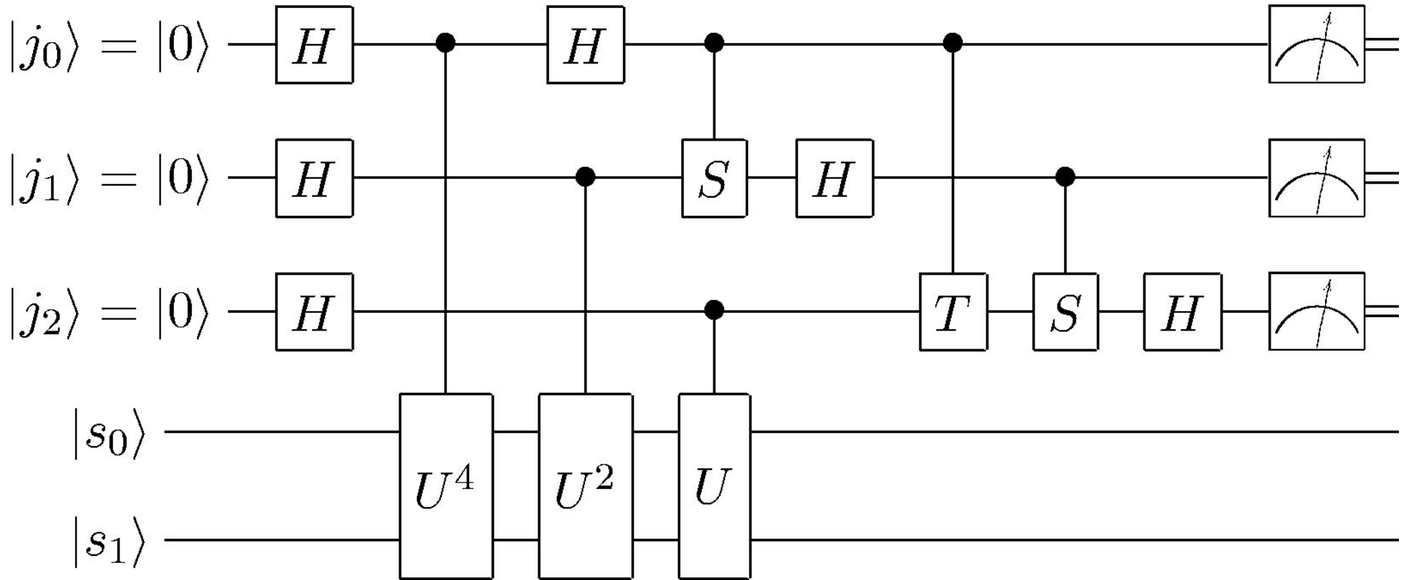
- Built ground-up for Quantum
- Support for Windows, macOS, and Linux
- Fully integrated into Visual Studio and VS Code
- Interoperability with Python (Windows only)
- Native type system




Learn Quantum Computation using Qiskit


IBM
Associate Certified
Developer
Quantum Computation using Qiskit v0.2X


python


$|j_0\rangle = |0\rangle$
$|j_1\rangle = |0\rangle$
$|j_2\rangle = |0\rangle$
$|s_0\rangle$
$|s_1\rangle$
H
H
H
H
S
H
T
S
H
U^4
U^2
U


Quantum Computing in Practice with Qiskit® and IBM Quantum Experience®
Packt

GOOGLE

Open Source - v 0.1 - 2018
Apache-2.0
Bibliotecas e documentos GitHub
Pyton

IBM

Open Source - v 0.1. 2017
Apache-2.0
Bibliotecas e documentos GitHub
Pyton + OpenQASM

MICROSOFT

QDK
Quantum Developed Kit

Open Source - v 0.1 - 2018
MIT
Bibliotecas e documentos GitHub
Q#

RIGETTI

Open Source - v 0.0.2 -. 2017
Apache-2.0
Bibliotecas e documentos GitHub
Pyton + Quil -> pyQuil

Considerações finais

PARA O FUTURO PRÓXIMO

Muito evolução deve vir pela frente:

Correção de erro
Armazenamento
Quântico
Repetidores quânticos
Maior capacidade de processamento

Desenvolvimento e Capacitação Técnica

Preparar pessoas para?

Desenvolvimento
Manutenção
Operação

Papel do Brasil ?

Desenvolvedor

ou

Somente consumidor

Referência para Desenvolvimento e Simulação

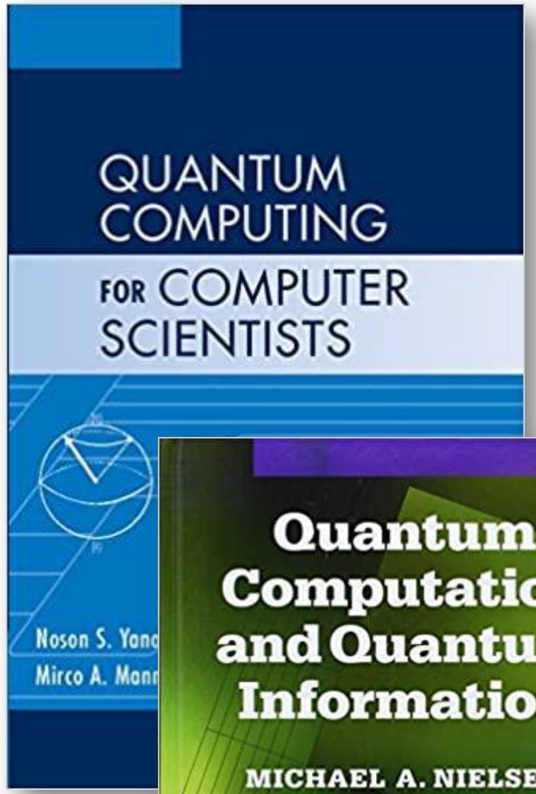
Google - CIRQ
https://github.com/quantumlib/Cirq

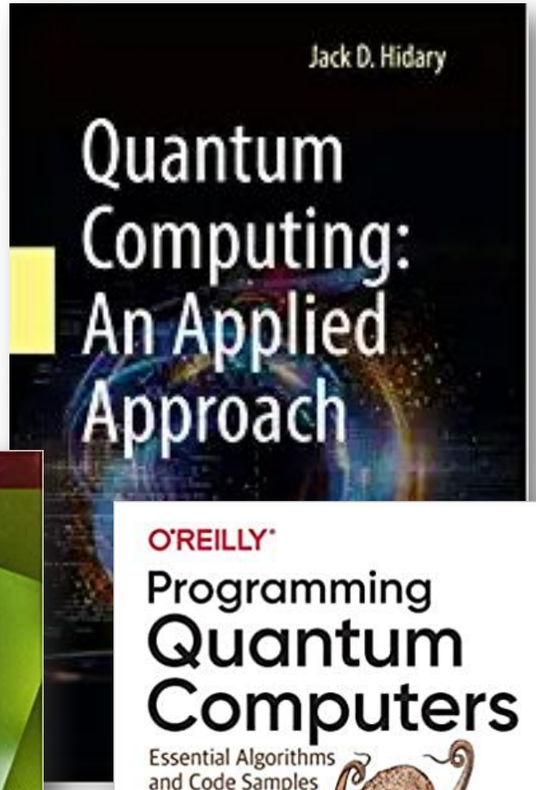
IBM - QisKit
https://qiskit.org/
https://github.com/Qiskit

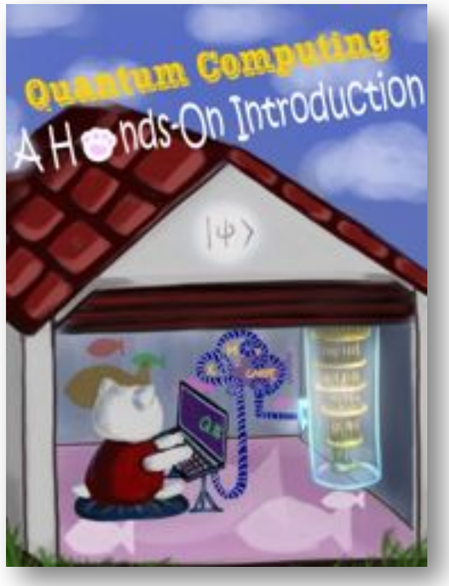
RIGETTI - Forest
https://www.rigetti.com/forest
https://github.com/rigetti/pyquil

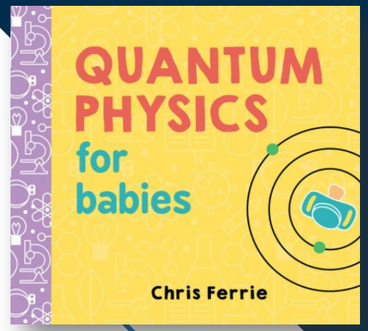
Microsoft - QDK
http://microsoft.com/en-us/quantum/development-kit
https://github.com/Microsoft/Quantum

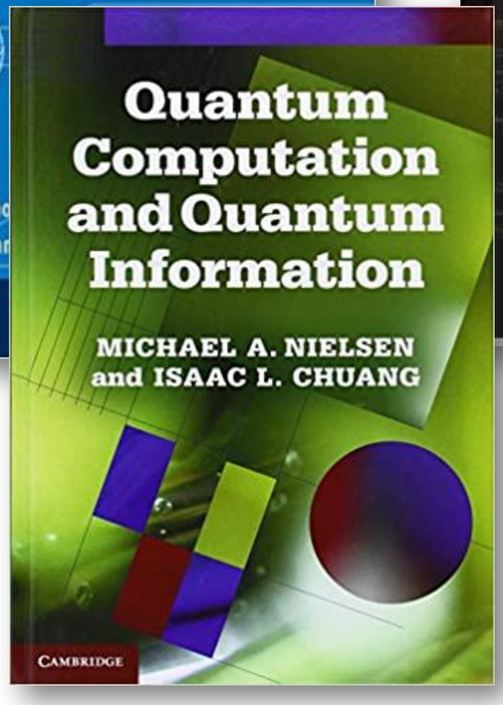
Referências

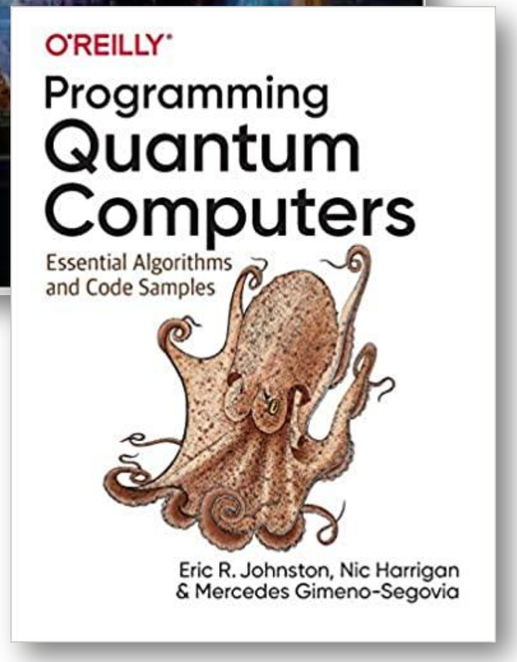


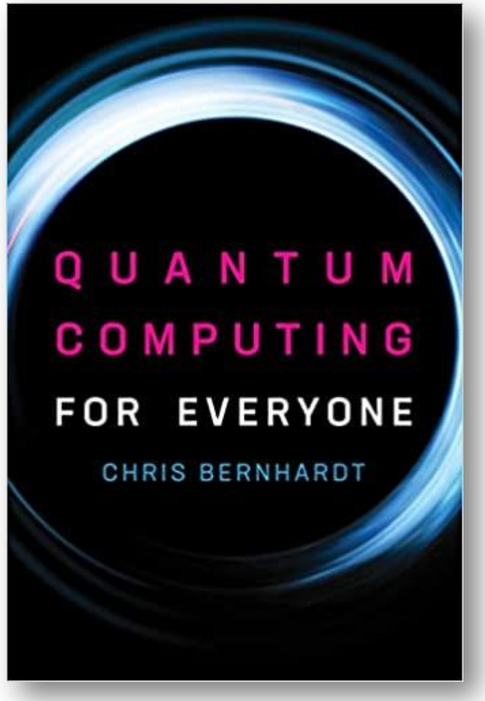


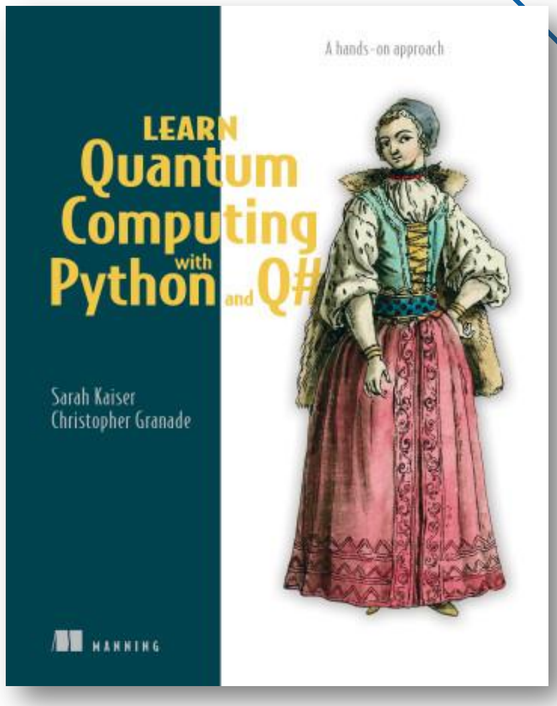












Obrigada!

regina@larc.usp.br