

(*) IBM's quantum device. Source: Wikipedia
(CC BY 4.0)

Computação quântica: progressos recentes e desafios

Franklin de Lima Marquezino
Universidade Federal do Rio de Janeiro
franklin@cos.ufrj.br

A revolução da computação quântica

- **Trata-se de usar a mecânica quântica para resolver problemas mais eficientemente**
- **Não é mágica: nem todo problema fica eficiente em computadores quânticos**

Os limites da computação clássica

Lei de Moore

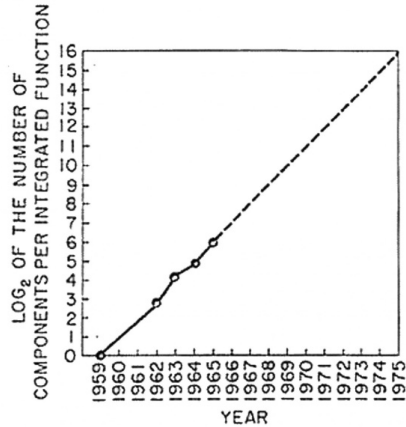


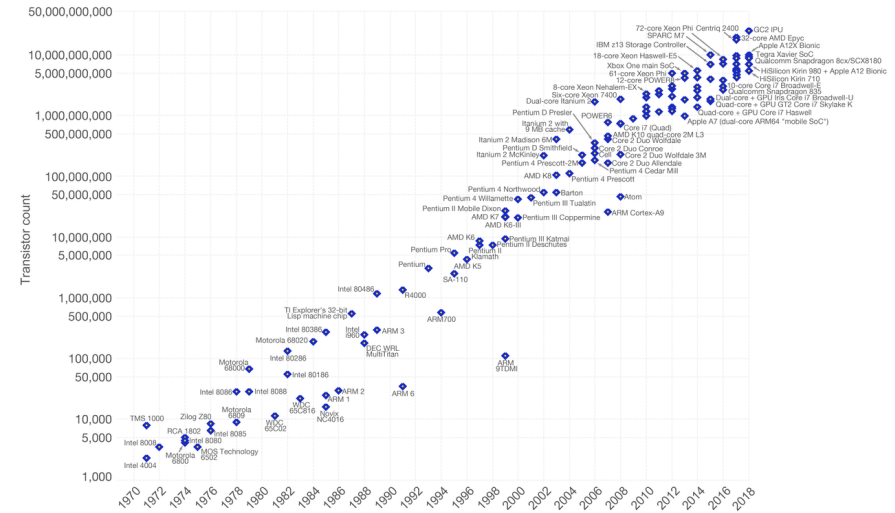
Fig. 2 Number of components per Integrated function for minimum cost per component extrapolated vs time.

(*) Gordon Moore's original graph, Source: Electronics, 1965



Moore's Law – The number of transistors on integrated circuit chips (1971-2018)
Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important as other aspects of technological progress – such as processing speed or the price of electronic products – are linked to Moore's law.

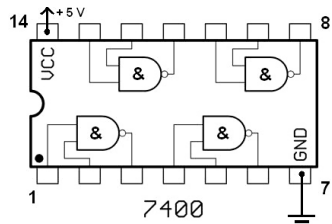
OurWorld
in Data



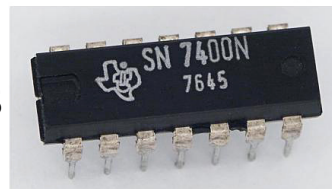
Data source: Wikipedia (https://en.wikipedia.org/wiki/Transistor_count)
The data visualization is available at OurWorldinData.org. There you find more visualizations and research on this topic.

Licensed under CC-BY-SA by the author Max Roser.

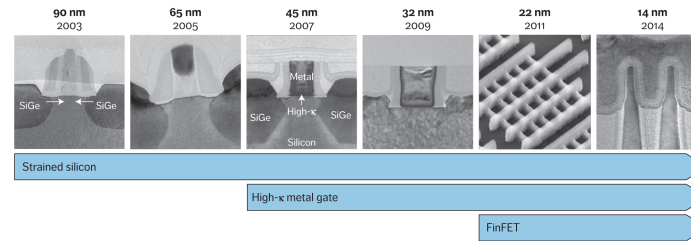
Miniaturização



1960s



(*) Texas IC containing 4 NAND gates. Source: Wikipedia



(*) Source: IEEE Micro, www.computer.org

2015



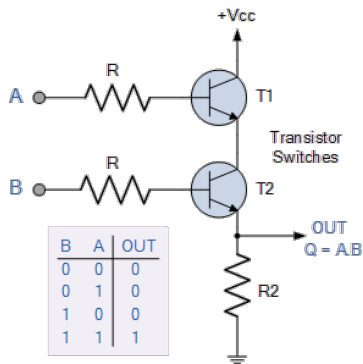
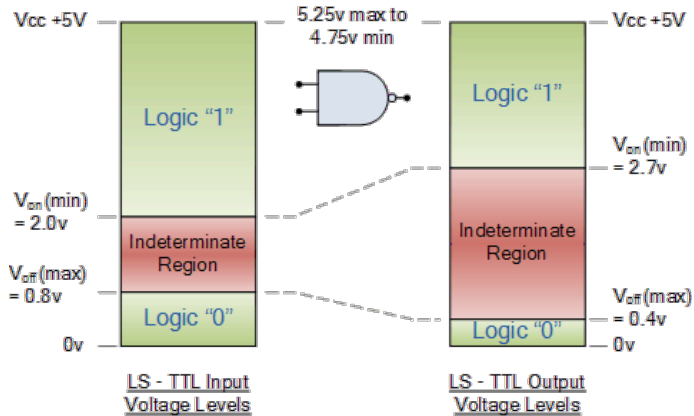
Mecânica quântica

- **Conselho para estudantes: Fiquem Calmos e Aprendam Álgebra Linear**
- **As regras do jogo, ou seja, os postulados da mecânica quântica**
 - ▷ Representação
 - ▷ Evolução
 - ▷ Medições
 - ▷ Composição



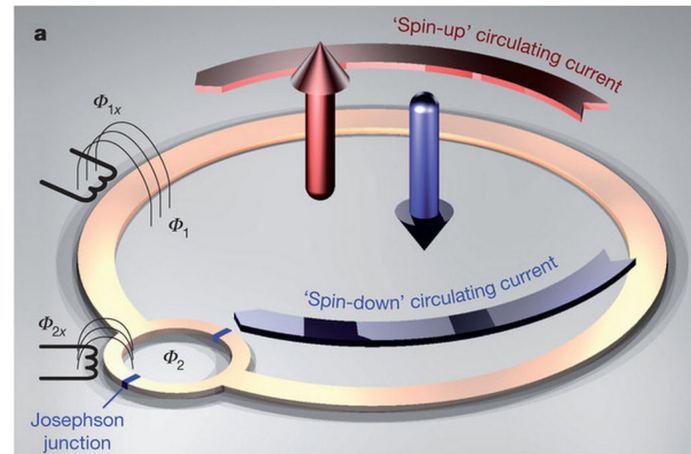
Apresentando os bits quânticos

- Bits (clássicos) podem ser 0 ou 1



(*) Source: www.electronics-tutorials.ws

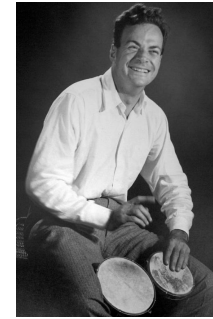
- Bits quânticos (qubits) pode ser um vetor (1,0) ou um vetor (0,1) ou qualquer combinação deles



(*) Superconducting qubit. Source: "Quantum annealing with manufactured spins", Nature, 2011

Breve histórico da computação quântica

- **1980 - P. Benioff and Y. Manin (em Russo): primeiras ideias**
- **1981 - Feynman: difícil simular MQ em computadores clássicos**
- **1994 - Algoritmo de Shor**
- **1996 - Algoritmo de Grover**
- **2001 - Número 15 fatorado com 7 qubits**
- **2016 - IBM Quantum Experience**



Aplicações de computadores quânticos

▪ Simulação

- Química quântica
- Design de materiais
- Design de fármacos

▪ Otimização

- Finanças
- Óleo & gás

▪ Machine learning

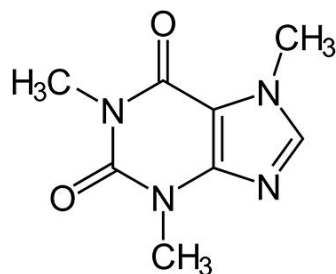
▪ Buscas

▪ Fatoração

▪ etc.

mais cedo

mais tarde



Simulação clássica, 10^{48} bits
(Mais que o número de átomos de nosso planeta!)

Simulação quântica, 160 qubits

**Quantum Computers
Destroy Internet Security**

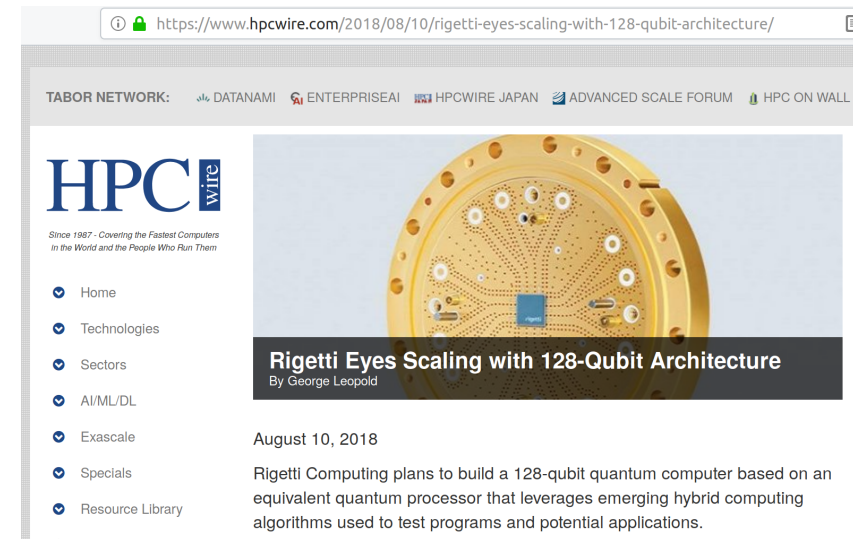
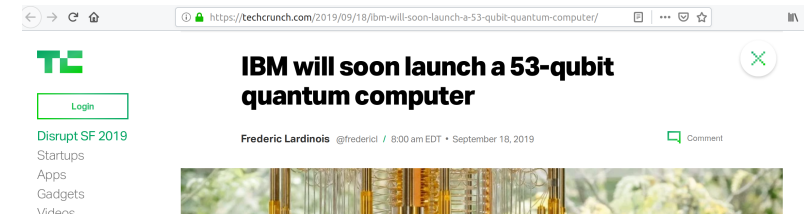


(*) minutephysics, Youtube

Requer muitos qubits e tolerância a falhas

Supremacia quântica

- **Usar um computador quântico para resolver um problema que não seja prático em um computador clássico**
- **Não precisa ser problema útil**
- **Candidatos**
 - Fatoração
 - Amostragem de circuitos quânticos aleatórios
 - Amostragem de bosons
- **Supremacia quântica será atingida em breve!**
 - Simulações usando computadores clássicos só vão até 56 qubits até hoje
 - 9 PB para simular 50 qubits, cada qubit adicional dobra o requisito



Computadores quânticos atuais

- **Posso rodar um programa quântico no meu computador de casa?**

- Não! Você pode simular, mas pode ser extremamente lento!

- **Você vai precisar de um computador quântico!**

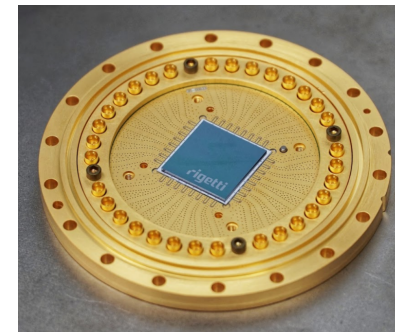
- **Já existem alguns computadores QREI disponíveis (poucos qubits, ruidosos)**

- IBM Q Experience

- Rigetti (precisa de convite)

- Dwave Leap (não no Brasil)

- **Vários outros já foram anunciados**



Empresas

Software e consultoria



QILIMANJARO

|EeroQ>

Hardware quântico



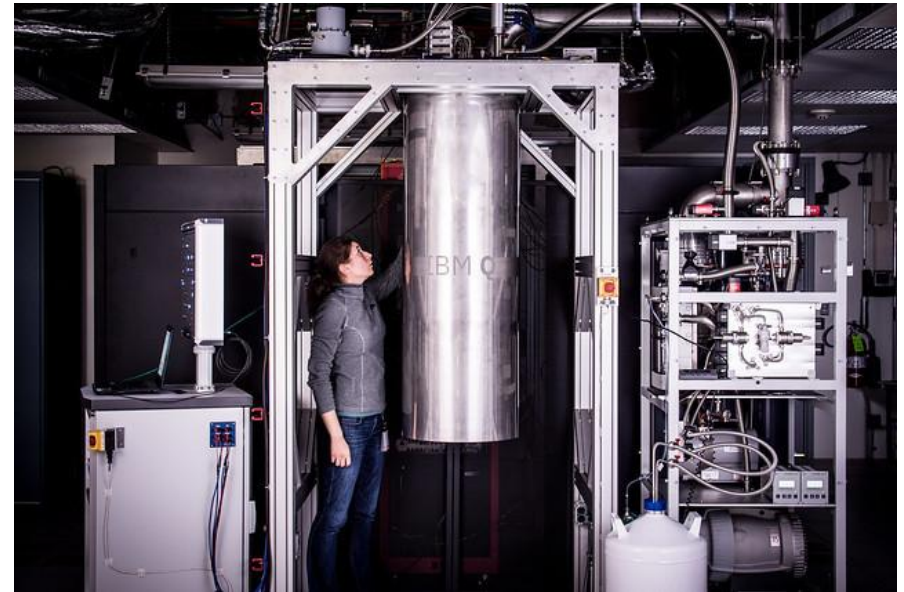
... and many others

Programando um computador quântico

- **IBM: circuit composer, Qasm, Qiskit (Python)**
- **Rigetti: Forest (Python)**
- **Xanadu: PennyLane (Python)**
- **Dwave: Ocean (Python)**
- **Microsoft: Q#**
- **Outros: ProjectQ, Qubiter, etc**

IBM Quantum Experience

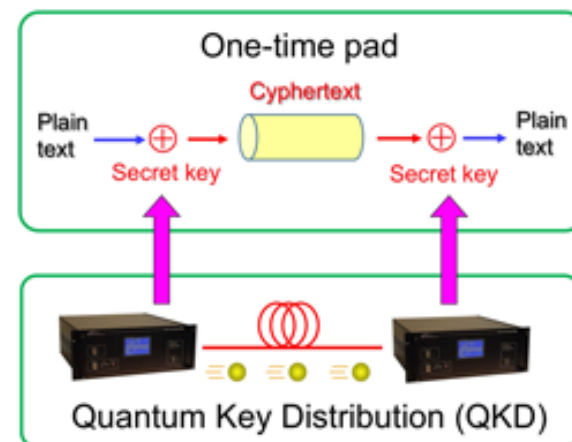
- **Boa oportunidade para experimentar computadores QREI**
- **Sistemas premium**
 - ▷ IBM Q Tokyo (20 qubits)
- **Sistemas públicos**
 - ▷ IBM Q Melbourne (14 qubits)
 - ▷ IBM Q Tenerife (5 qubits)
 - ▷ IBM Q Yorktown (5 qubits)
 - ▷ IBM Q Ourense (5 qubits)
 - ▷ IBM Q Vigo (5 qubits)
 - ▷ IBM QASM Simulator (até 32 qubits simulados)



(*) IBM Research

Consequências para criptografia

- **CQ quebra RSA (mas requer muitos qubits)**
- **Motiva a criptografia pós-quântica**
- **Novas oportunidades para troca de chaves e comunicação segura**



(*) Source: www.nict.go.jp



(*) Source: physicsworld.com

Como ingressar nessa área

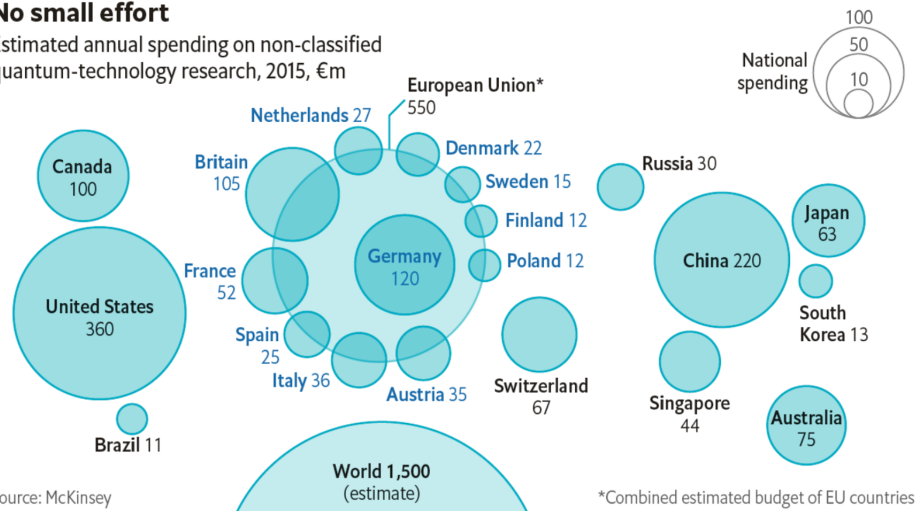
- **Graduação: matemática, computação, engenharia, física etc (várias possibilidades)**
- **Muita atenção aos cursos de Álgebra Linear**
- **Aprenda a programar os computadores quânticos da IBM (github programaquantica)**
- **Iniciação científica: ideal iniciar o quanto antes**
- **Mestrado/Doutorado: UFRJ/COPPE/PESC**
 - ▷ **Inscrições estão abertas!**
<http://www.cos.ufrj.br/selecao>

Conclusão

- **Supremacia quântica: poucos anos**
- **Vantagem quântica, impacto em negócios: 5-10 anos**
- **Escala completa, tolerância a falhas: 10-20 anos**
- **Muitas oportunidades na academia e na indústria**

No small effort

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



Source: McKinsey

The New York Times

The Next Tech Talent Shortage: Quantum Computing Researchers

By Cade Metz

Oct. 21, 2018

Christopher Savoie, founder and chief executive of a start-up called Zapata, offered jobs this year to three scientists who specialize in an increasingly important technology called quantum computing. They accepted.

Several months later, the Cambridge, Mass., company was still waiting for the State

Para saber mais

- **Webinar RNP**

<https://esr.rnp.br/webinar/computacaoquantica>

- **Apostila**

<https://github.com/programaquantica>

- **Palestra do Prof. Ulisses Mello (IBM) no Youtube**

Obrigado!

Computação quântica: progressos recentes e desafios

Franklin de Lima Marquezino
Univeresidade Federal do Rio de Janeiro
franklin@cos.ufrj.br