ConFLOSS

2021

Q
(Computação Quântica
+
Comunidade Open Source)

em superposição

Daniele Nazaré

Quem Sou Eu?

Eu sou uma nerd e autoditada, apaixonada por tecnologia, cinema, livros, ciência **[*E muito Doida*]**. Estuda Engenharia de Computação no Inatel, e faço parte da organização do Flisol Santa Rita do Sapucaí.

Contato

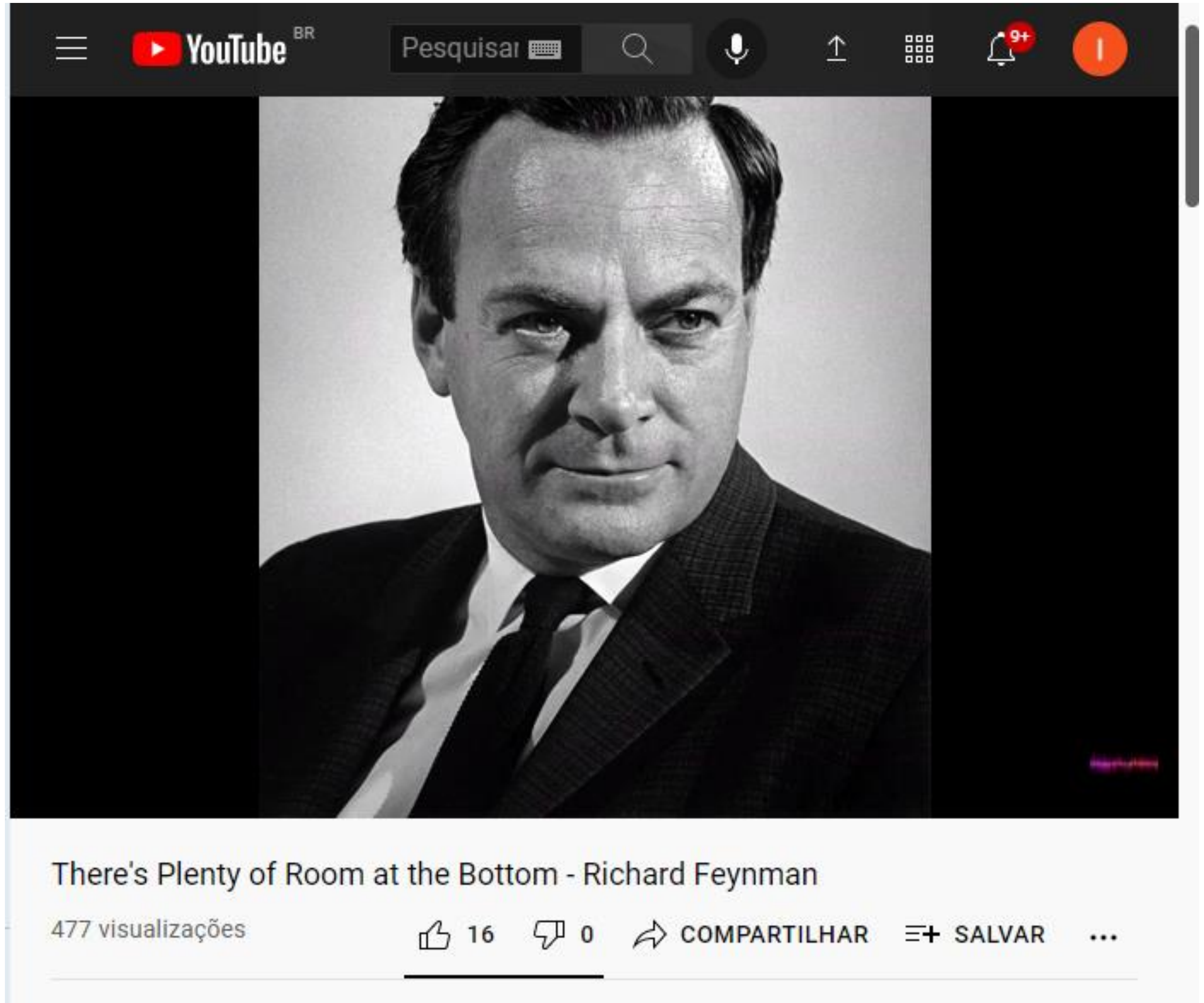
Dany.nt.14@gmail.com

https://github.com/danynt14

https://www.linkedin.com/in/danielenazare/


Intro

Quem idealizou a possibilidade de processamento de dados com a mecânica quântica?



"Há muito espaço no Fundo" [1959]

https://www.youtube.com/watch?v=DSDEUYNujxU

Quem idealizou a possibilidade de processamento de dados com a mecânica quântica?

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

1. INTRODUCTION

On the program it says this is a keynote speech—and I don't know what a keynote speech is. I do not intend in any way to suggest what should be in this meeting as a keynote of the subjects or anything like that. I have my own things to say and to talk about and there's no implication that anybody needs to talk about the same thing or anything like it. So what I want to talk about is what Mike Dertouzos suggested that nobody would

http://physics.whu.edu.cn/dfiles/wenjian/1_00_QIC_Feynman.pdf

David Deusch

Propôs a ideia de Computador Quântico Universal

[1985]

Quando o interesse em Computação Quântica aumentou?

[1994]

Algorithms for Quantum Computation: Discrete Log and Factoring

Extended Abstract

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974 USA

email: shor@research.att.com

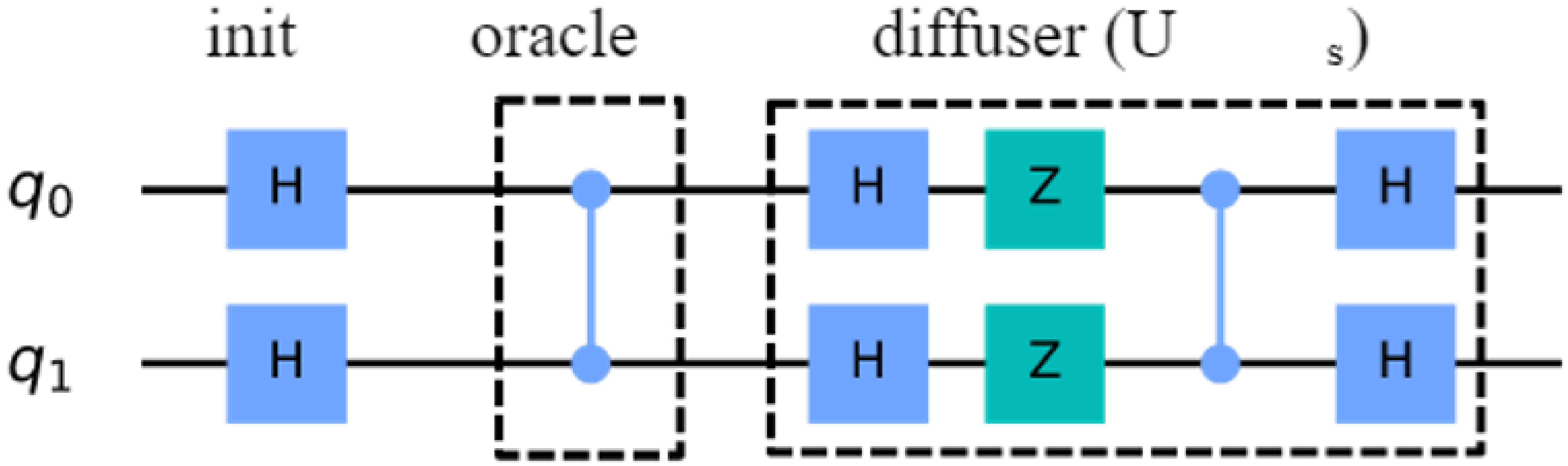
Abstract

This paper gives algorithms for the discrete log and the factoring problems that take random polynomial time on a quantum computer (thus giving the first examples of quantum cryptanalysis).

Lov K. Grover

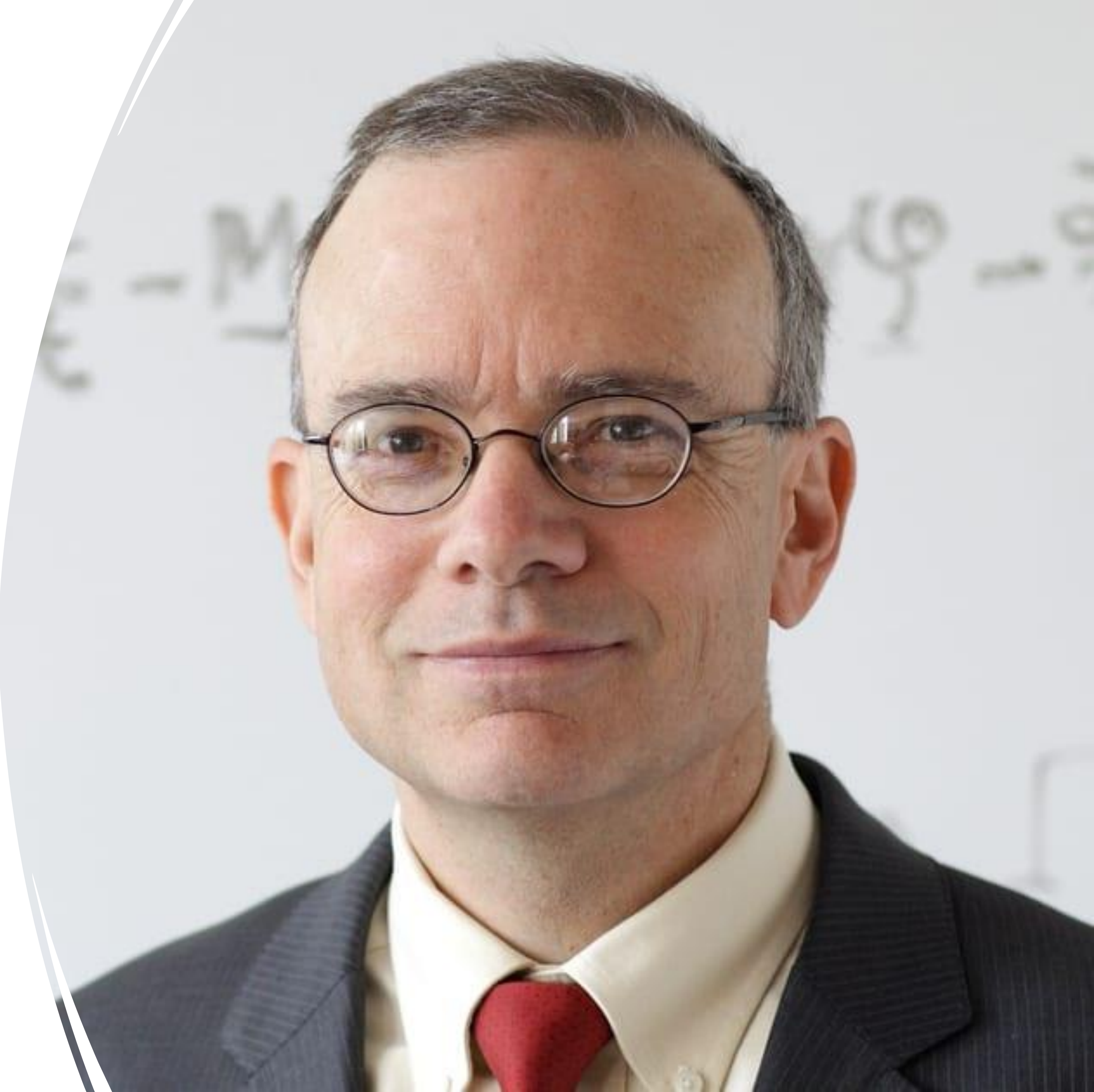
Algoritmo de busca *O(n1/2)*

Ou Algoritmo de Groover [1996]



D'Vincenzo

Definiu os critérios para se ter um computador quântco [1996]



Empresas

IBM

HUAWEI

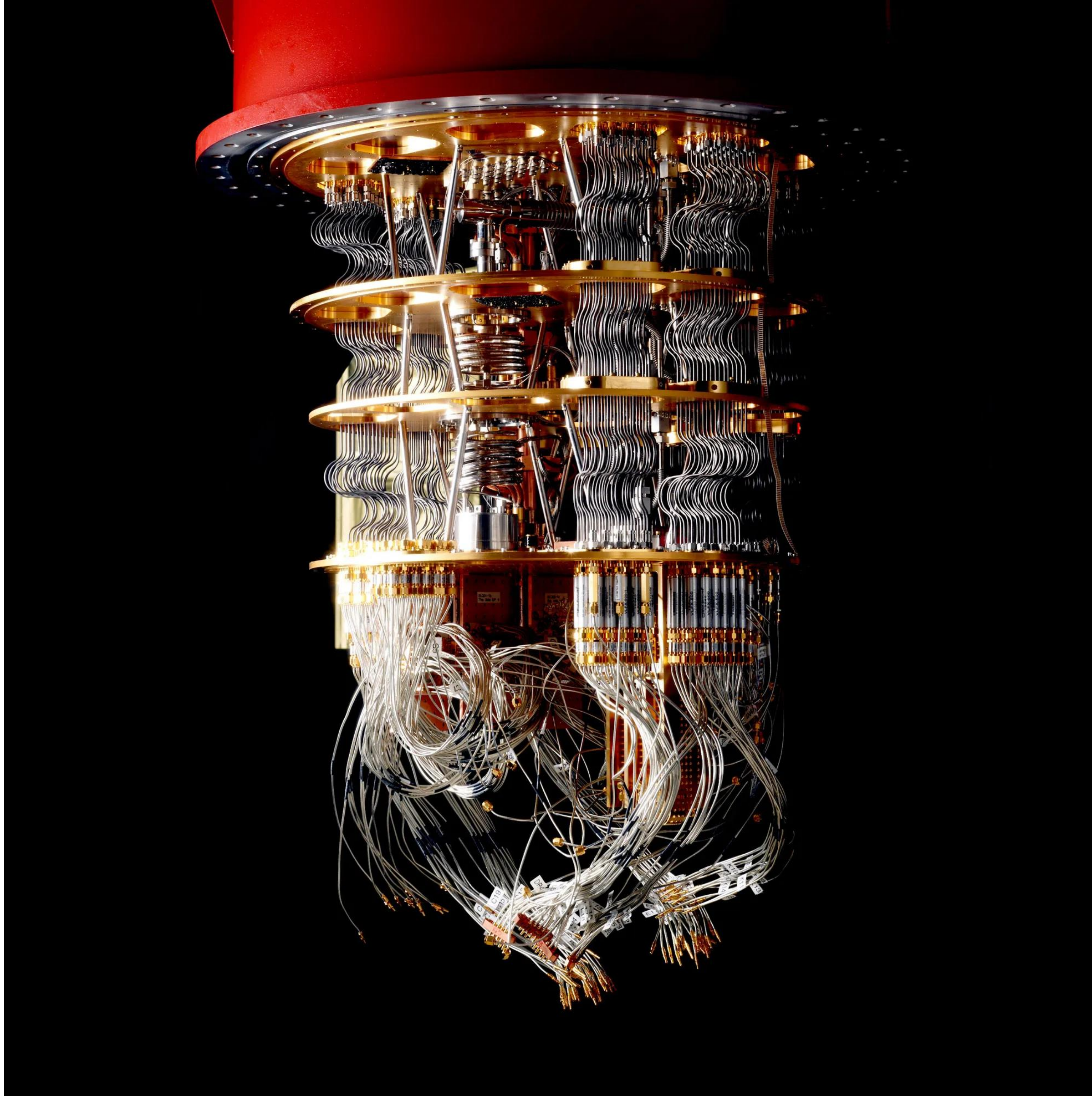
accenture

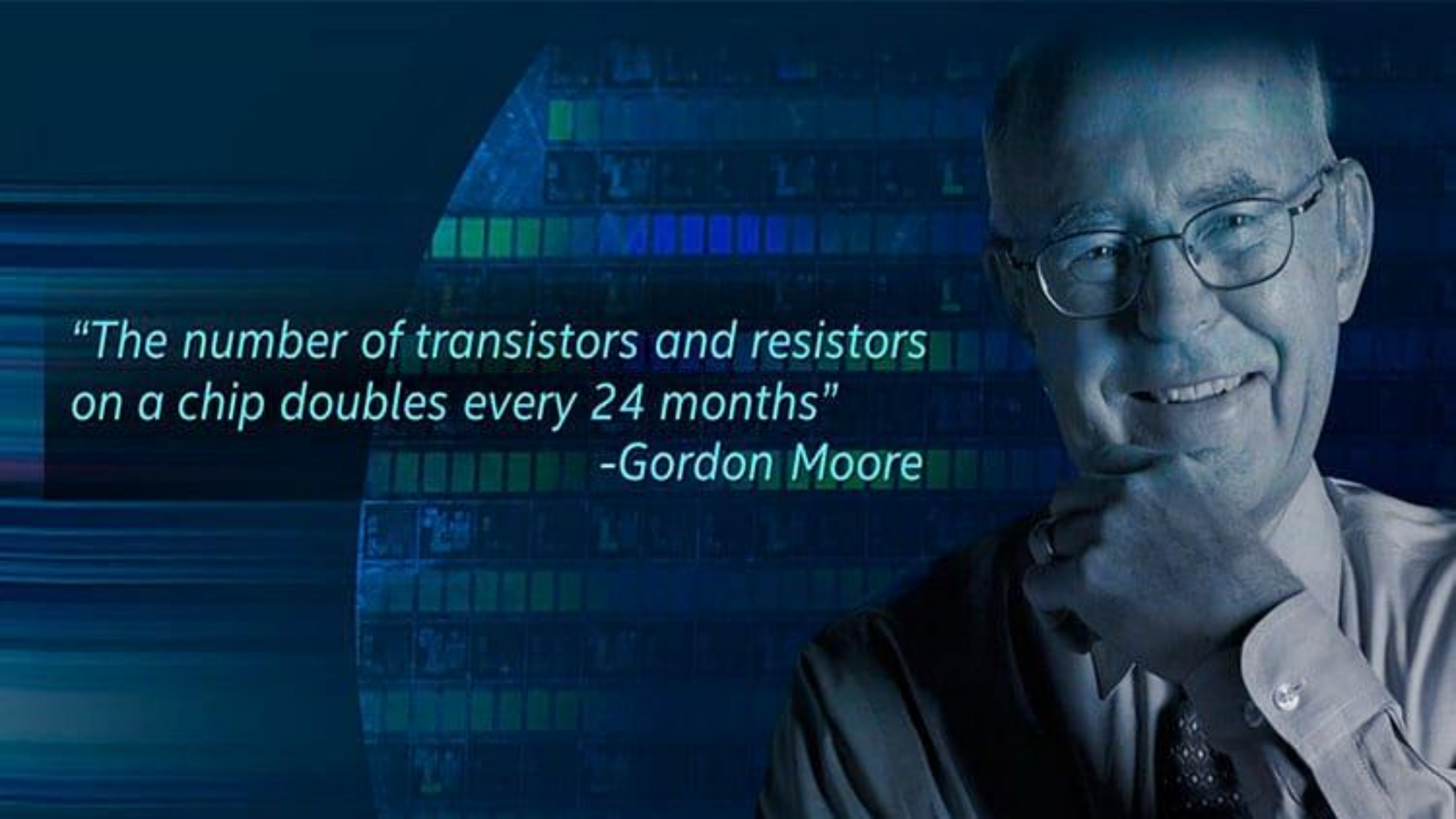
Google

D:Wave
The Quantum Computing Company™

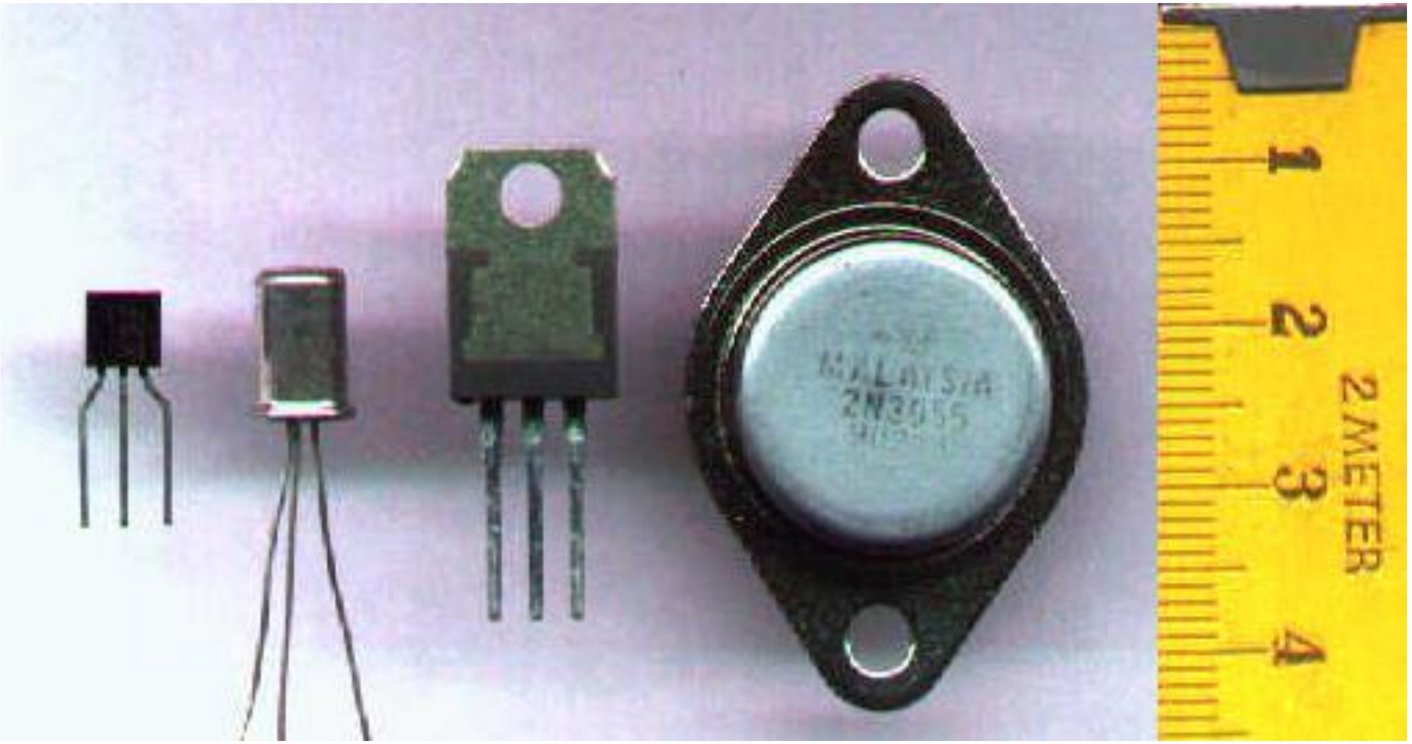
Microsoft

Por que Computação Quântica?

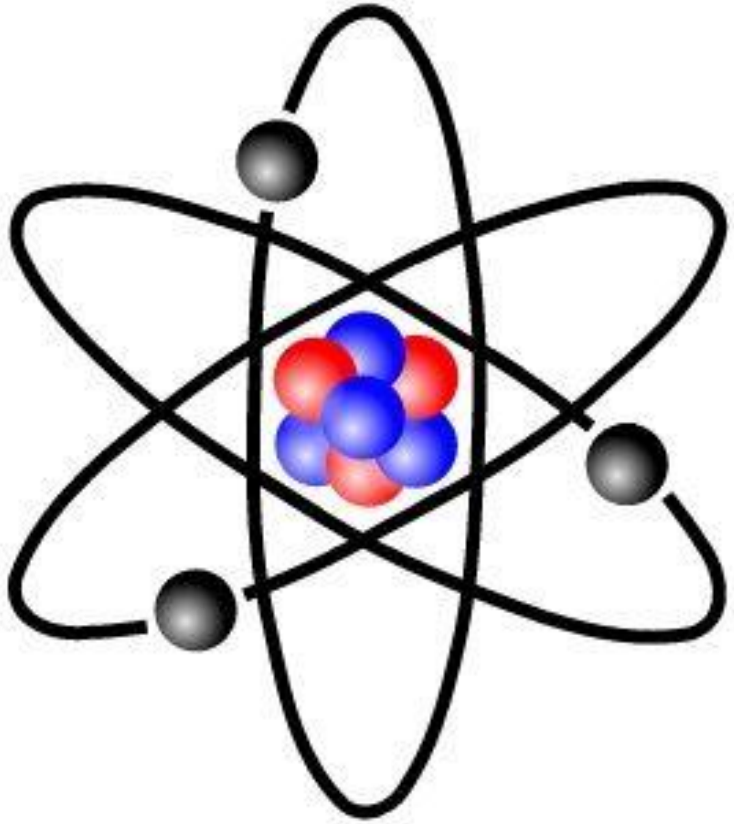



“The number of transistors and resistors
on a chip doubles every 24 months”
-Gordon Moore

Miniatuarização do Transistor



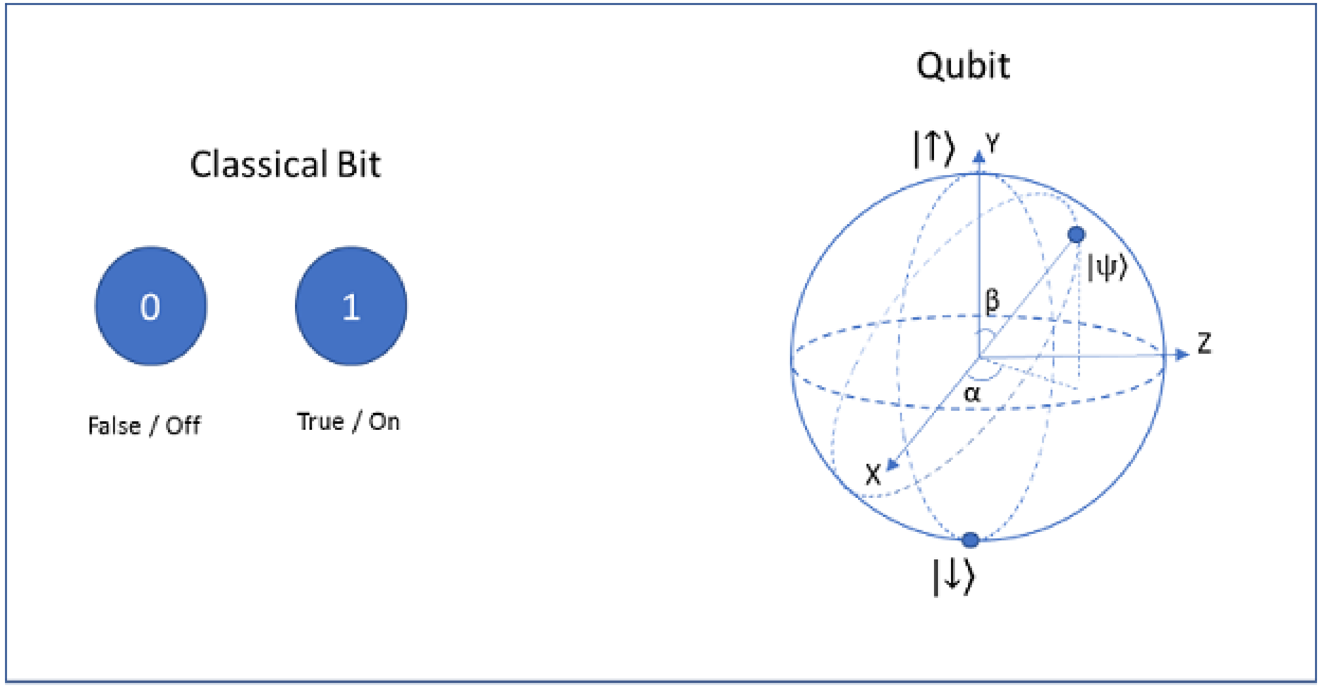
Miniatuarização do Transistor



Velocidade da Luz = 299 792 458 m / s

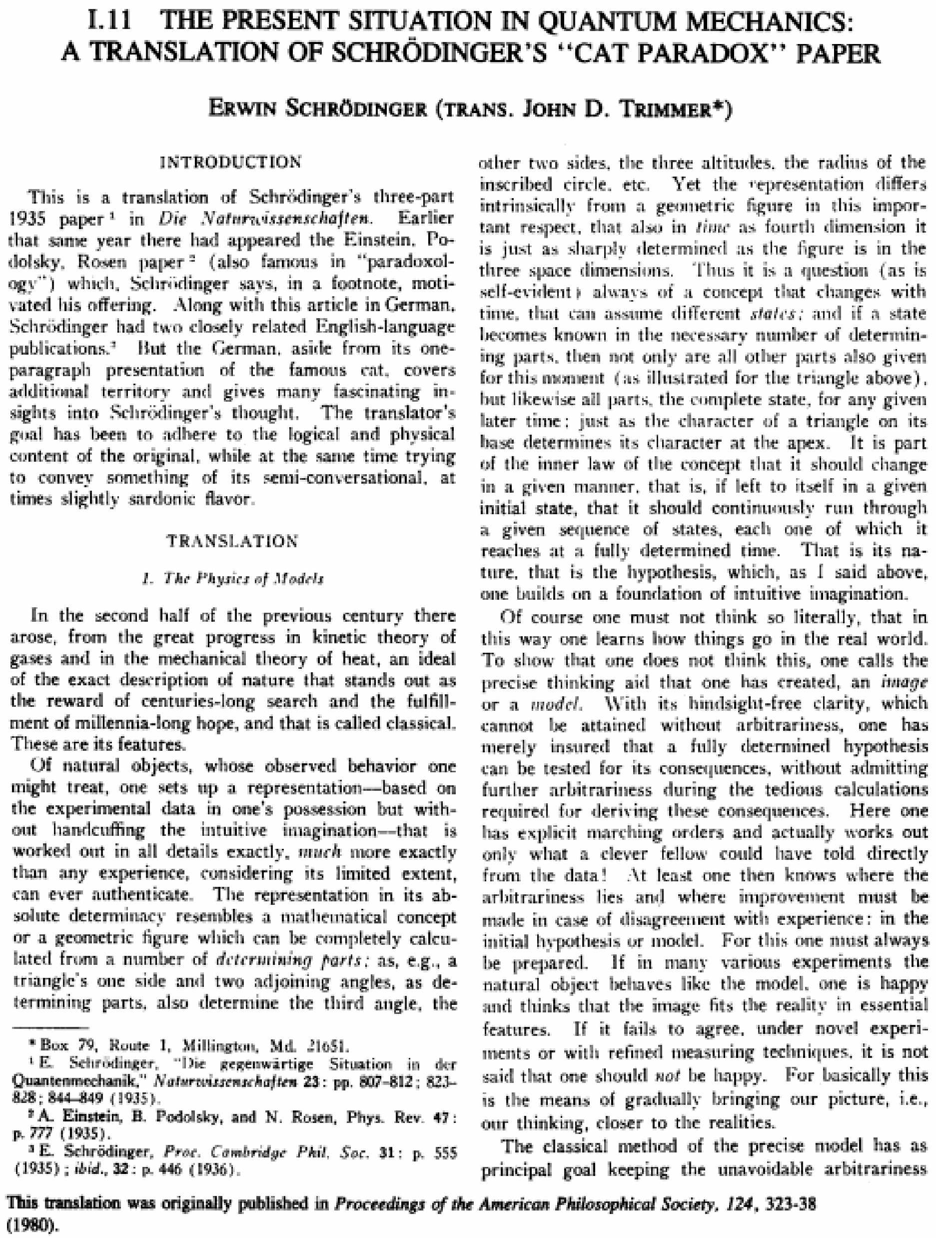
Computação Quântica

Bit vs. quBit



Computação Quântica

Experimento do Gato de Schrödinger[35]



I.11 THE PRESENT SITUATION IN QUANTUM MECHANICS: A TRANSLATION OF SCHRÖDINGER'S "CAT PARADOX" PAPER

ERWIN SCHRÖDINGER (TRANS. JOHN D. TRIMMER*)

INTRODUCTION

This is a translation of Schrödinger's three-part 1935 paper[1] in *Die Naturwissenschaften*. Earlier that same year there had appeared the Einstein, Podolsky, Rosen paper[2] (also famous in "paradoxology") which, Schrödinger says, in a footnote, motivated his offering. Along with this article in German, Schrödinger had two closely related English-language publications.[3] But the German, aside from its one-paragraph presentation of the famous cat, covers additional territory and gives many fascinating insights into Schrödinger's thought. The translator's goal has been to adhere to the logical and physical content of the original, while at the same time trying to convey something of its semi-conversational, at times slightly sardonic flavor.

TRANSLATION

1. The Physics of Models

In the second half of the previous century there arose, from the great progress in kinetic theory of gases and in the mechanical theory of heat, an ideal of the exact description of nature that stands out as the reward of centuries-long search and the fulfillment of millennia-long hope, and that is called classical. These are its features.

Of natural objects, whose observed behavior one might treat, one sets up a representation—based on the experimental data in one's possession but without handcuffing the intuitive imagination—that is worked out in all details exactly, *much* more exactly than any experience, considering its limited extent, can ever authenticate. The representation in its absolute determinacy resembles a mathematical concept or a geometric figure which can be completely calculated from a number of *determining parts*; as, e.g., a triangle's one side and two adjoining angles, as determining parts, also determine the third angle, the other two sides, the three altitudes, the radius of the inscribed circle, etc. Yet the representation differs intrinsically from a geometric figure in this important respect, that also in *time* as fourth dimension it is just as sharply determined as the figure is in the three space dimensions. Thus it is a question (as is self-evident) always of a concept that changes with time, that can assume different *states*; and if a state becomes known in the necessary number of determining parts, then not only are all other parts also given for this moment (as illustrated for the triangle above), but likewise all parts, the complete state, for any given later time; just as the character of a triangle on its base determines its character at the apex. It is part of the inner law of the concept that it should change in a given manner, that is, if left to itself in a given initial state, that it should continuously run through a given sequence of states, each one of which it reaches at a fully determined time. That is its nature, that is the hypothesis, which, as I said above, one builds on a foundation of intuitive imagination.

Of course one must not think so literally, that in this way one learns how things go in the real world. To show that one does not think this, one calls the precise thinking aid that one has created, an *image* or a *model*. With its hindsight-free clarity, which cannot be attained without arbitrariness, one has merely insured that a fully determined hypothesis can be tested for its consequences, without admitting further arbitrariness during the tedious calculations required for deriving these consequences. Here one has explicit marching orders and actually works out only what a clever fellow could have told directly from the data! At least one then knows where the arbitrariness lies and where improvement must be made in case of disagreement with experience: in the initial hypothesis or model. For this one must always be prepared. If in many various experiments the natural object behaves like the model, one is happy and thinks that the image fits the reality in essential features. If it fails to agree, under novel experiments or with refined measuring techniques, it is not said that one should *not* be happy. For basically this is the means of gradually bringing our picture, i.e., our thinking, closer to the realities.

The classical method of the precise model has as principal goal keeping the unavoidable arbitrariness

* Box 79, Route 1, Millington, Md. 21651.

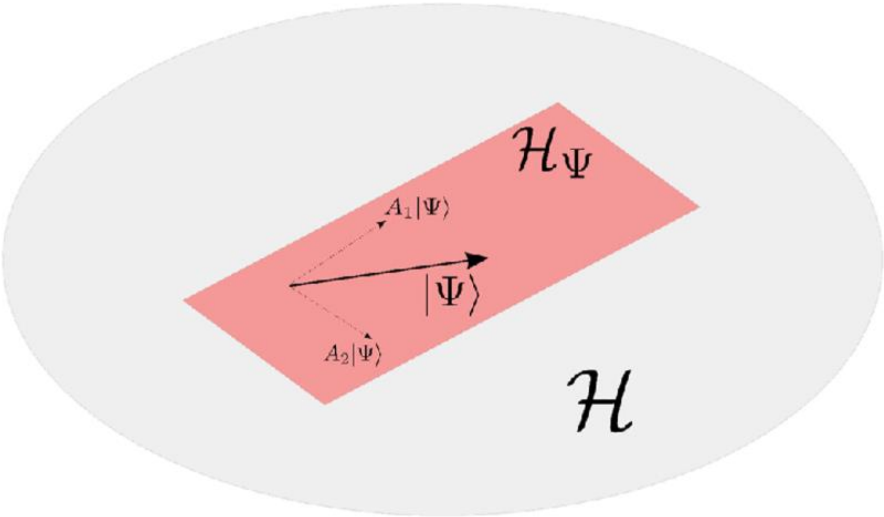
[1] E. Schrödinger, "Die gegenwärtige Situation in der Quantenmechanik," *Naturwissenschaften* **23**: pp. 807–812; 823–828; 844–849 (1935).

[2] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**: p. 777 (1935).

[3] E. Schrödinger, *Proc. Cambridge Phil. Soc.* **31**: p. 555 (1935); *ibid.*, **32**: p. 446 (1936).

This translation was originally published in *Proceedings of the American Philosophical Society, 124*, 323-38 (1980).

Computação
Clássica vs. Quântica



Álgebra Booleana
Mecânica Clássica
Caráter Determinístico
0 ou 1

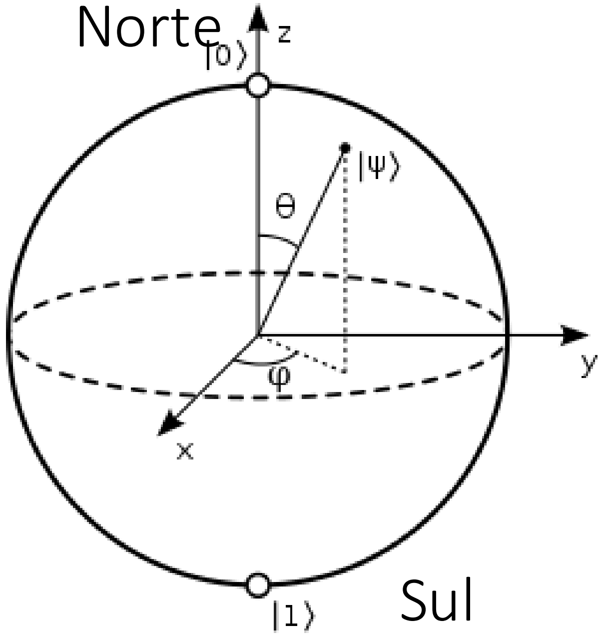
Espaço de Hilbert
Mecânica Quântica
Caráter Probabilístico
0 e 1

Computação Clássica vs. Quântica

0: Cara/ Falso

1: Coroa / Verdadeiro

0 / 1



Sobreposição de estados quânticos

Ket |ψ>

TABLE I
ILUSTRA A QUANTIDADE DE BITS QUE CADA QUBIT POSSUI .

quBit (n)	Bits (2^n)	Bytes
1	2	–
2	4	–
3	8	1
4	16	2
5	32	4
6	64	8
7	128	16
8	256	32
9	512	64
10	1024	128
15	32768	4096
20	1048576	131072
25	33554432	4194304
50	1.1258999e+15	1.4073749e+14
75	3.7778932e+22	4.7223665e+21
100	1.2676506e+30	1.5845633e+29

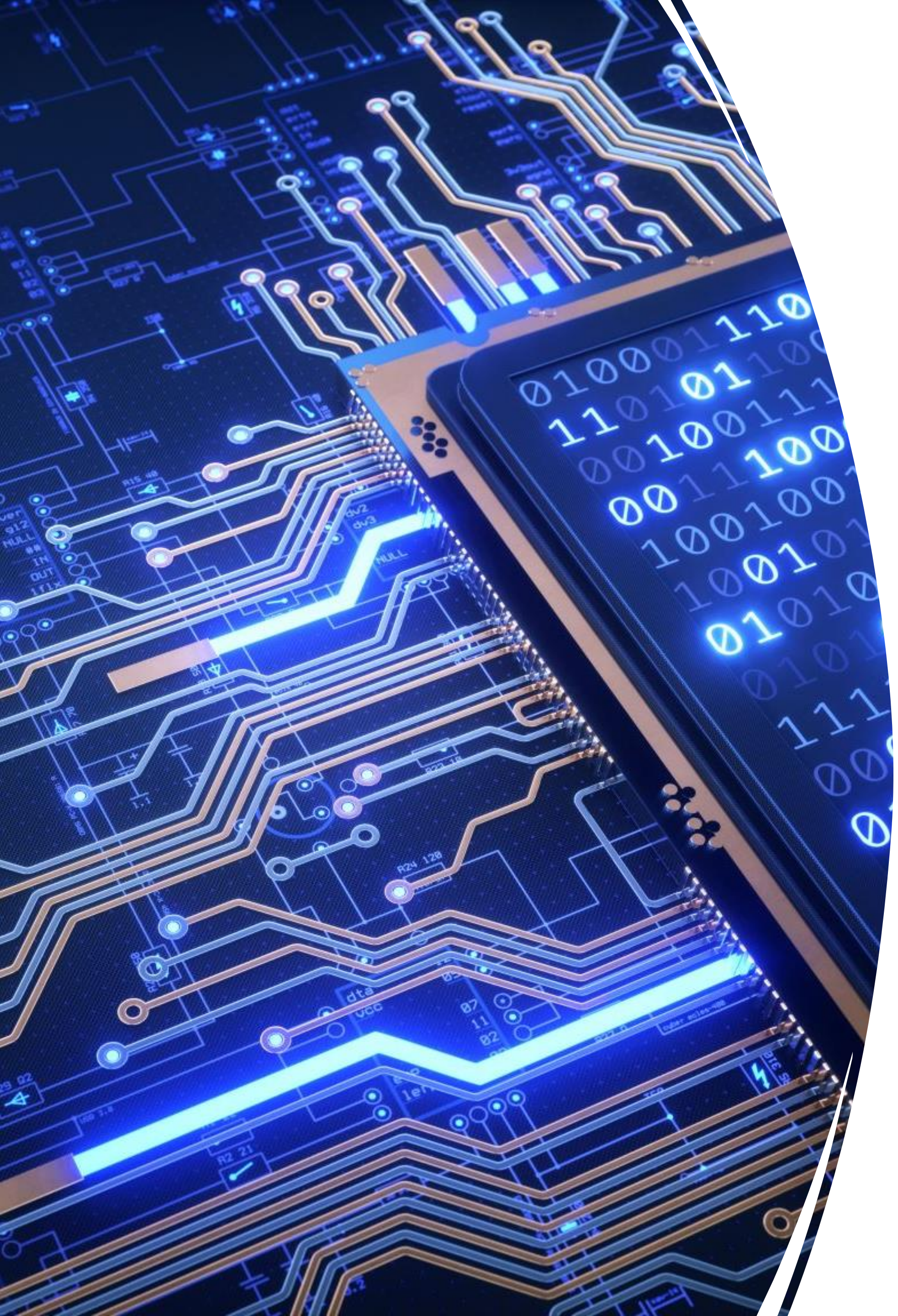
Na computação quântica, armazena-se
mais informações em regiões menores
e utiliza-se a álgebra linear
do Espaço de Hilbert
junto aos princípios lógicos de acordo com a propriedade
superposição de estados da mecânica quântica [19]

TABLE II

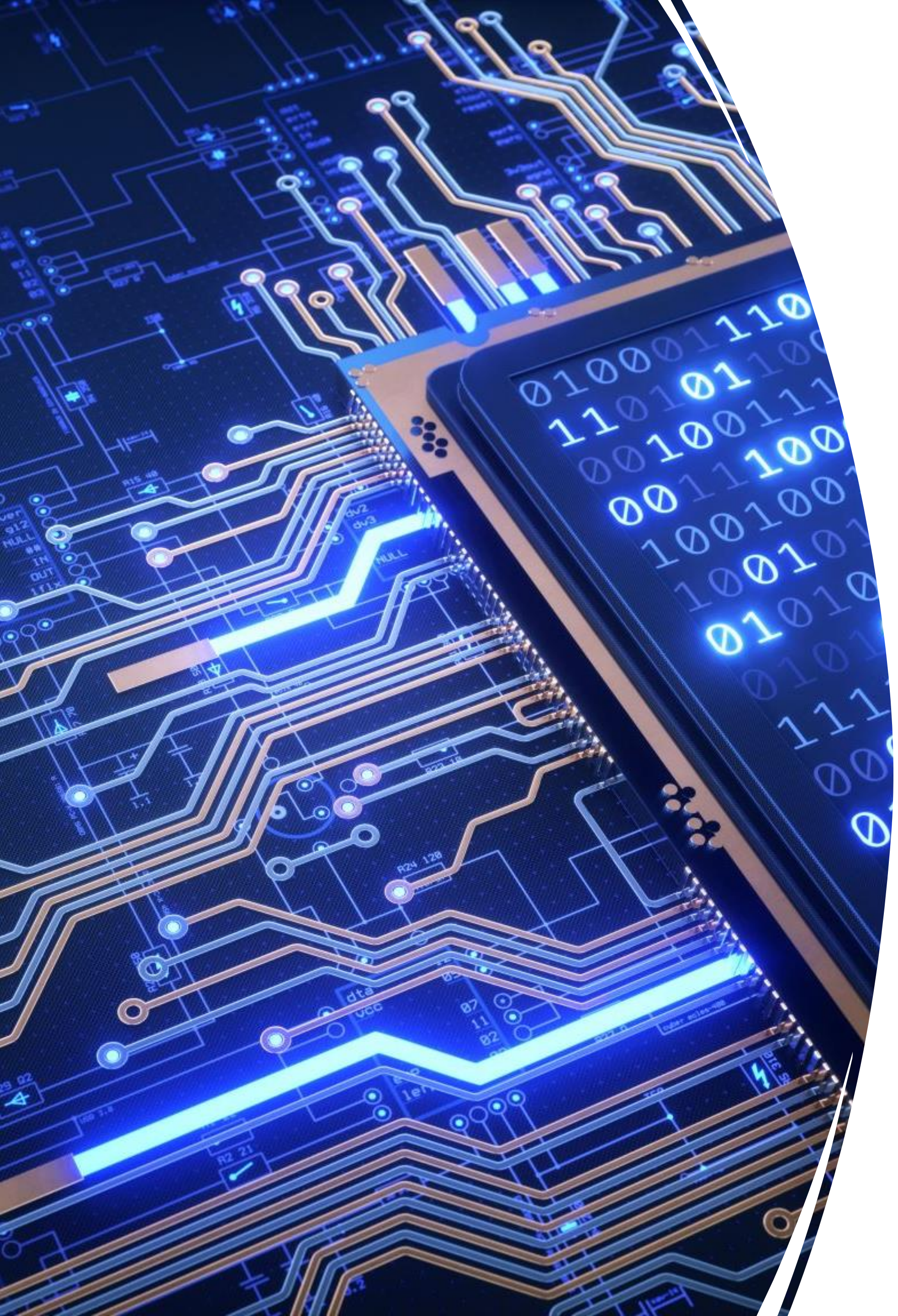
ILUSTRA PORTAS LÓGICAS QUÂNTICAS DE 1 QUBIT [23] .

Porta lógica	Representação Matemática	Representação Visual
Pauli-X	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	X
Pauli-Y	$\begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$	Y
Pauli-Z	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	Z
Hadamard	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	H
$\pi/8$ T	$\begin{pmatrix} 1 & 0 \\ 0 & \exp \frac{i\pi}{4} \end{pmatrix}$	T
S	$\begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$	S
CX	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	
CZ	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$	
SWAP	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	
Toffoli	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$	

Portas Lógicas



Será que teremos um computador quântico algum dia?



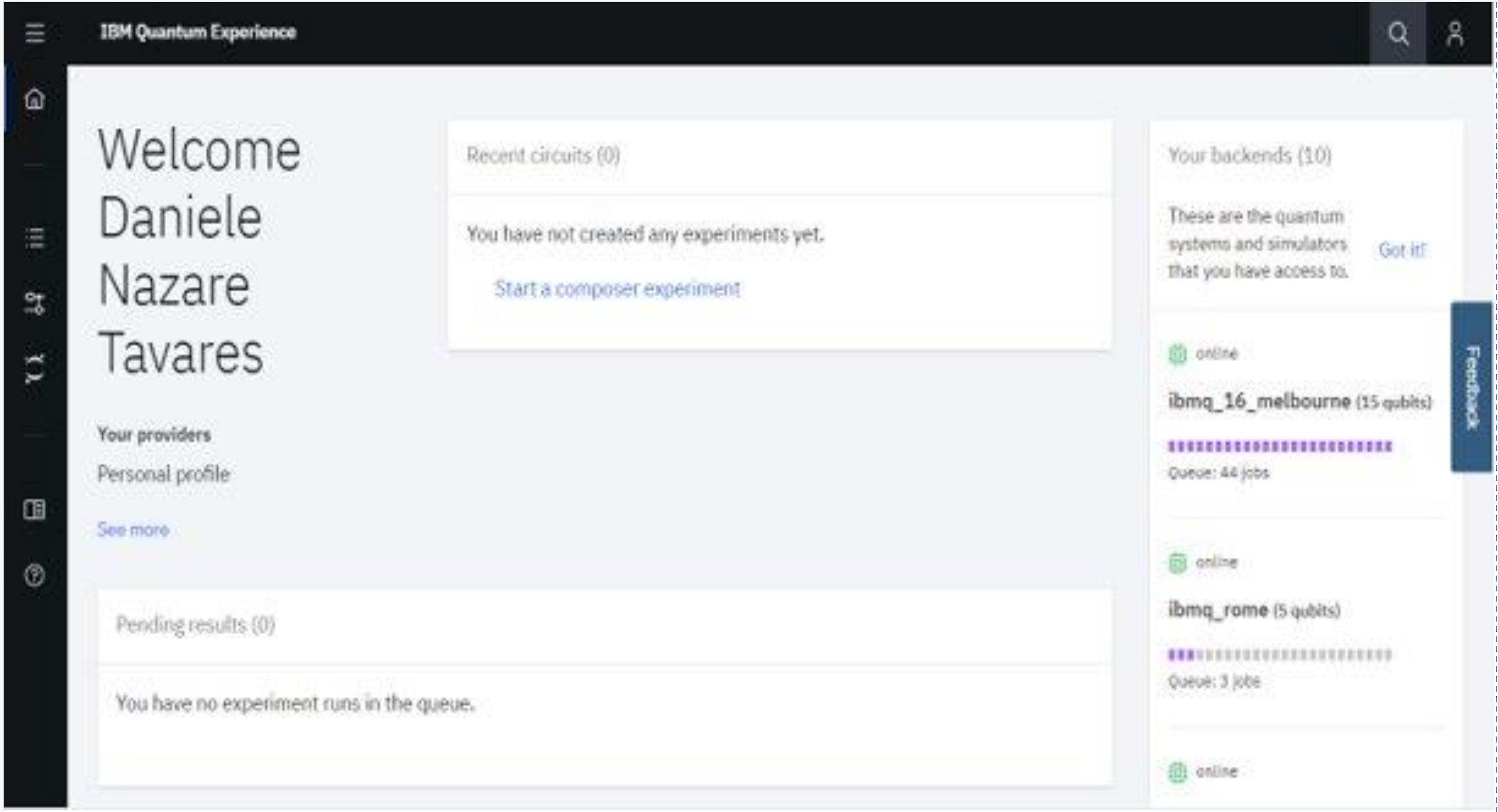
Será quee teremos um computador quântico algum dia?

Será precisaremos de um computador quântico?

Ferramentas de simulação e Linguagens

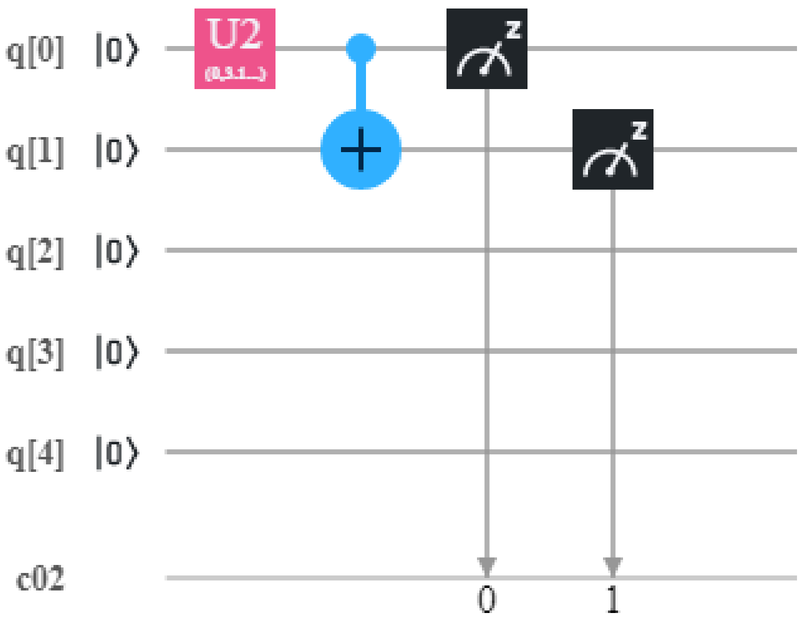
1. Qiskit
2. OpenQL
3. Q#
4. Silq
5. Braket
6. Cirq

IBM Quantum Experience

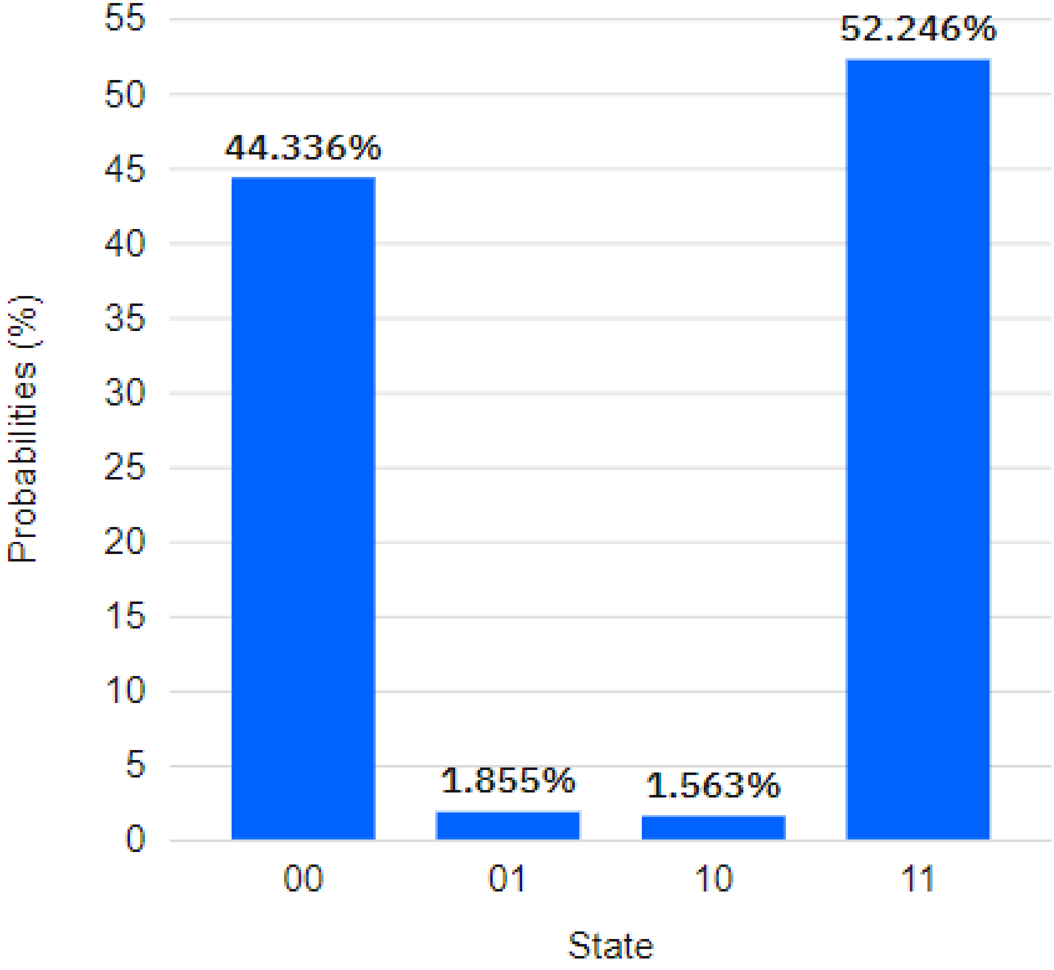


1. Circuit Composer **2. Qiskit Notebook** **3. Documentação**

Simulação

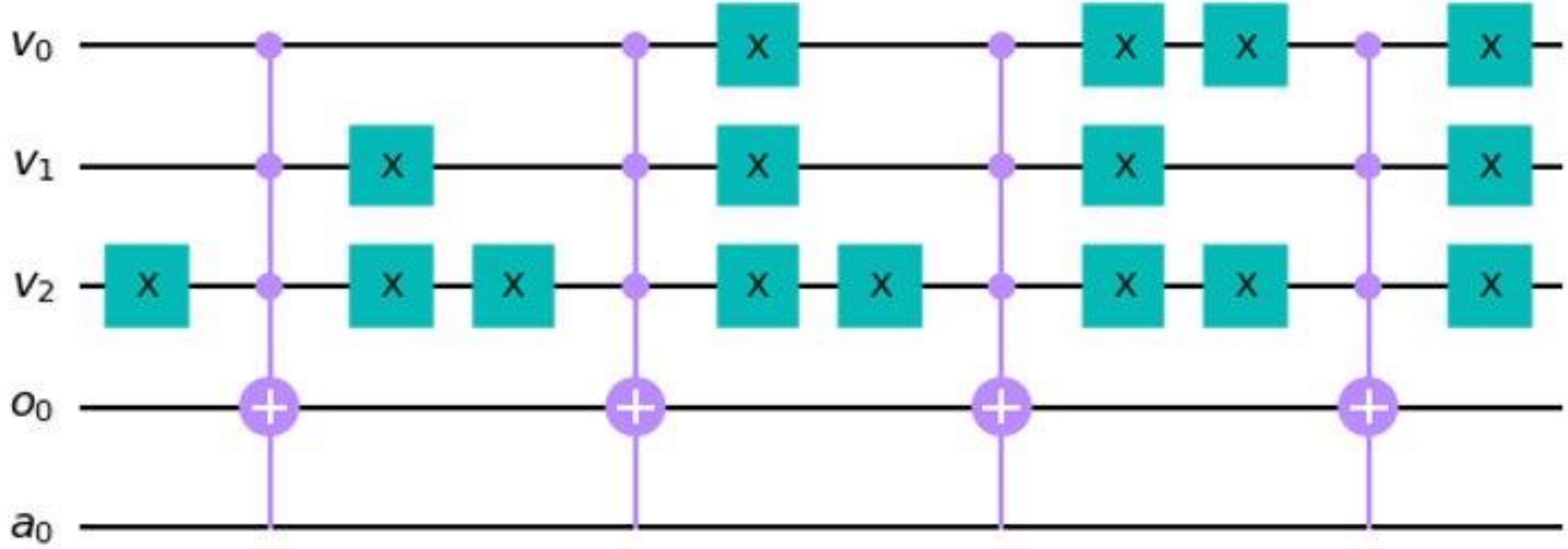


q[0] |0⟩
q[1] |0⟩
q[2] |0⟩
q[3] |0⟩
q[4] |0⟩
c02
U2
0
1



Probabilities (%)
55
50
45
40
35
30
25
20
15
10
5
0
44.336%
1.855%
1.563%
52.246%
00
01
10
11
State

Algoritmo de Shor



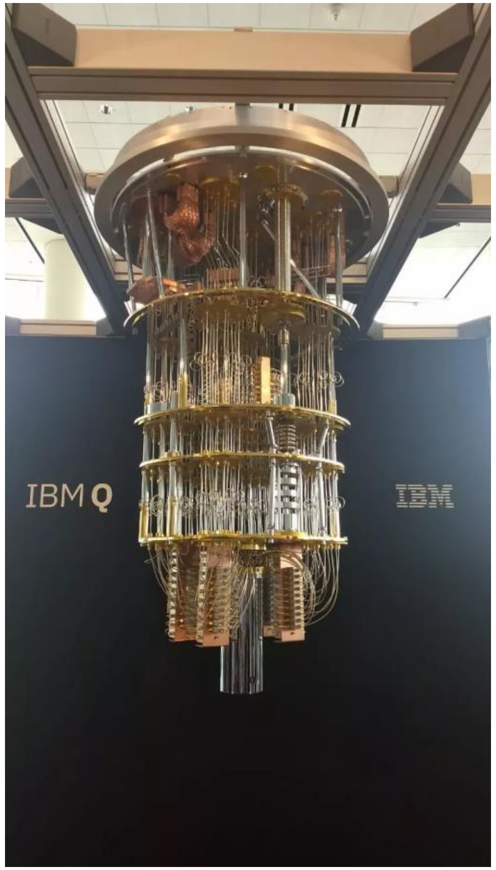
Caso especial da Computação!

Vulnerável a Ataques de um Computador Quântico!

RSA

Caso especial da Computação!

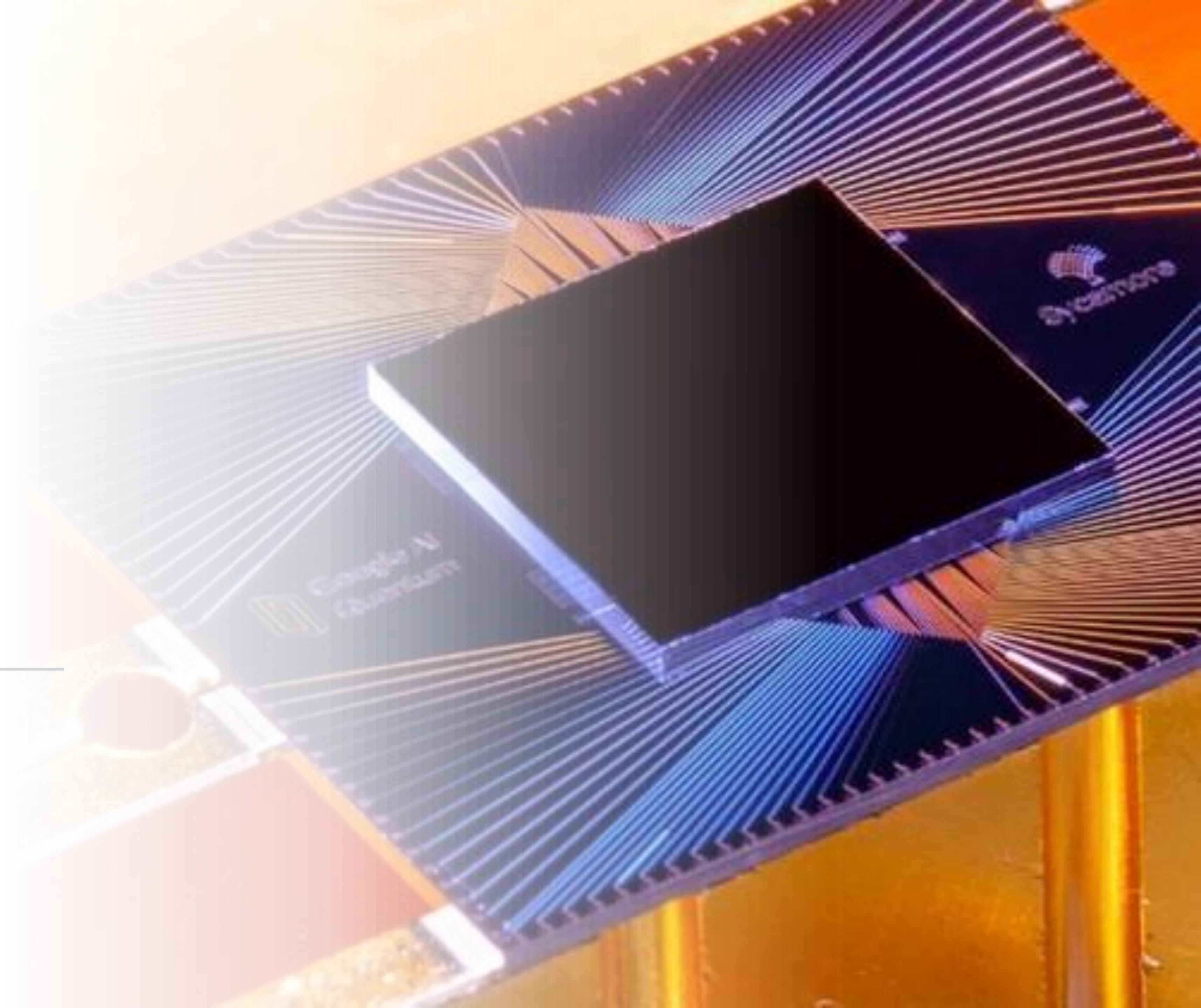
Maior Problema do Computador Quântico



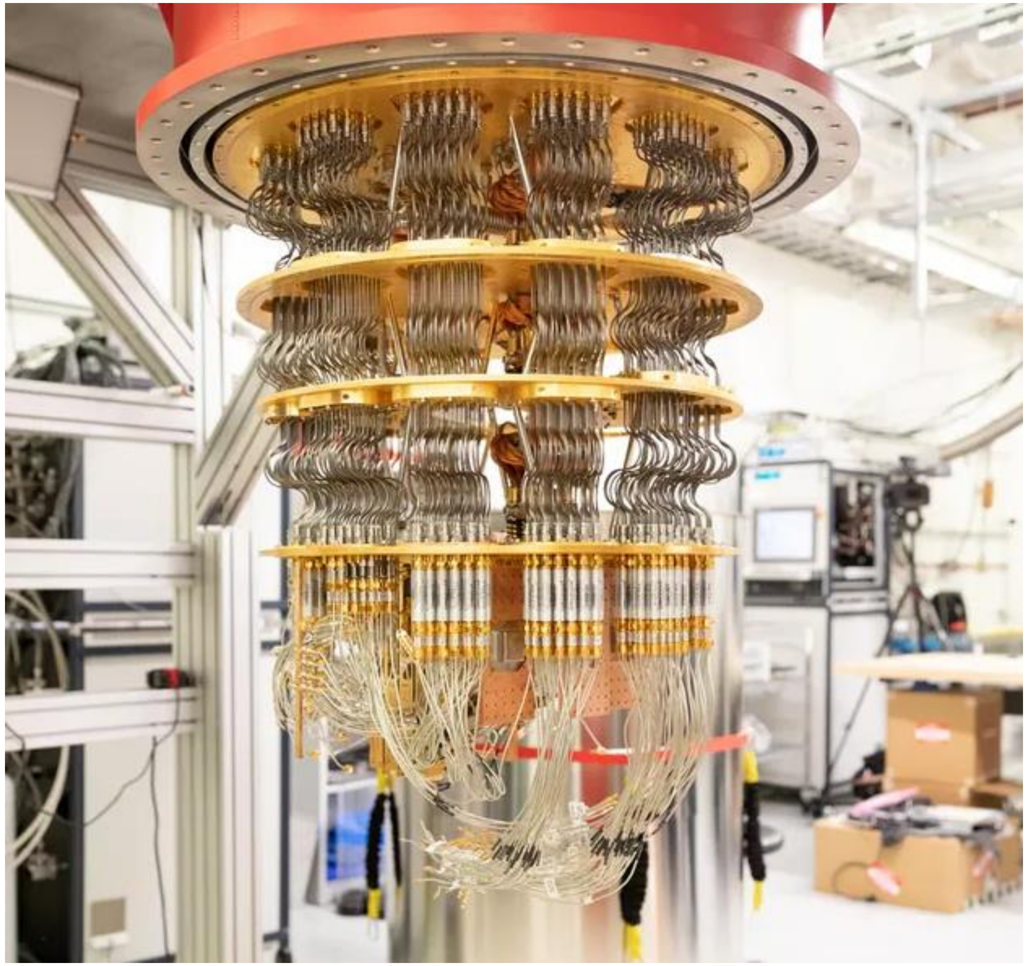
Isolamento Perfeito

O que é a **Supremacia Quântica?**

Google Images



Summit da IBM X Sycamore do Google



Summit da IBM X Sycamore do Google

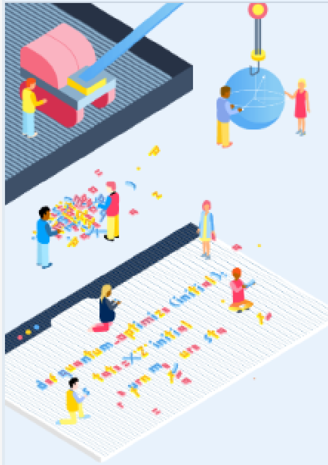
$f(x)$

10 mil anos X 3 minutos 20 segundos

qosf

HOME MANIFESTO LEARN CODE EVALUATION MENTORSHIP

Fork me on GitHub



Quantum Open Source Foundation

Supporting the development and standardization of open tools for quantum computing.

Become a supporter

Follow us on GitLab

Follow us on GitHub

THE TEAM →

Find out more about the team behind the Quantum Open Source Foundation (QOSF).

The QOSFoundation

What is open source?

Why you should open source.

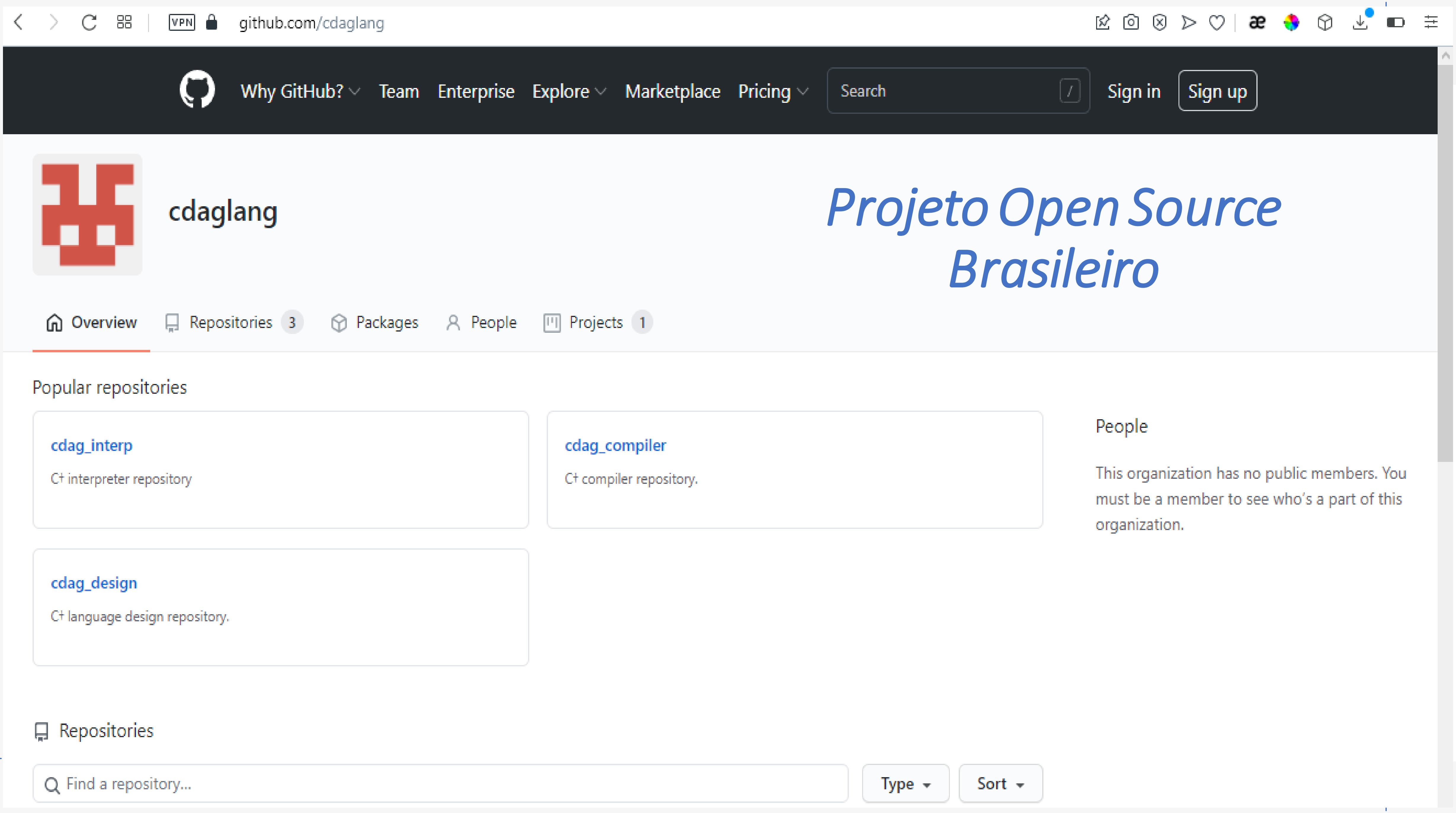
Quantum Open Source Fundation[QOSF]

- Expansão do papel de códigos abertos, a fim de melhorar sua padronização e qualidade.
- O foco principal do QOSF será no software destinado ao uso com tecnologias de computação quântica atuais e de curto prazo
  - Tecnologias quânticas de escala intermediária ruidosa (NISQ).

Quantum Open Source Fundation[QOSF]

- Promover integração de Comunidades de Hardware e Software
- Fornecer Financiamento
- Estimular a divulgação de conhecimento aberto em engenharia de software quântico e computação quântica
- Atravé de fóruns, reunir a comunidade para discutir problemas e soluções
- Organizar eventos como fóruns, conferências, meetups, bootcamp's, entre outros
- Transmitir conhecimento em engenharia de software quântico

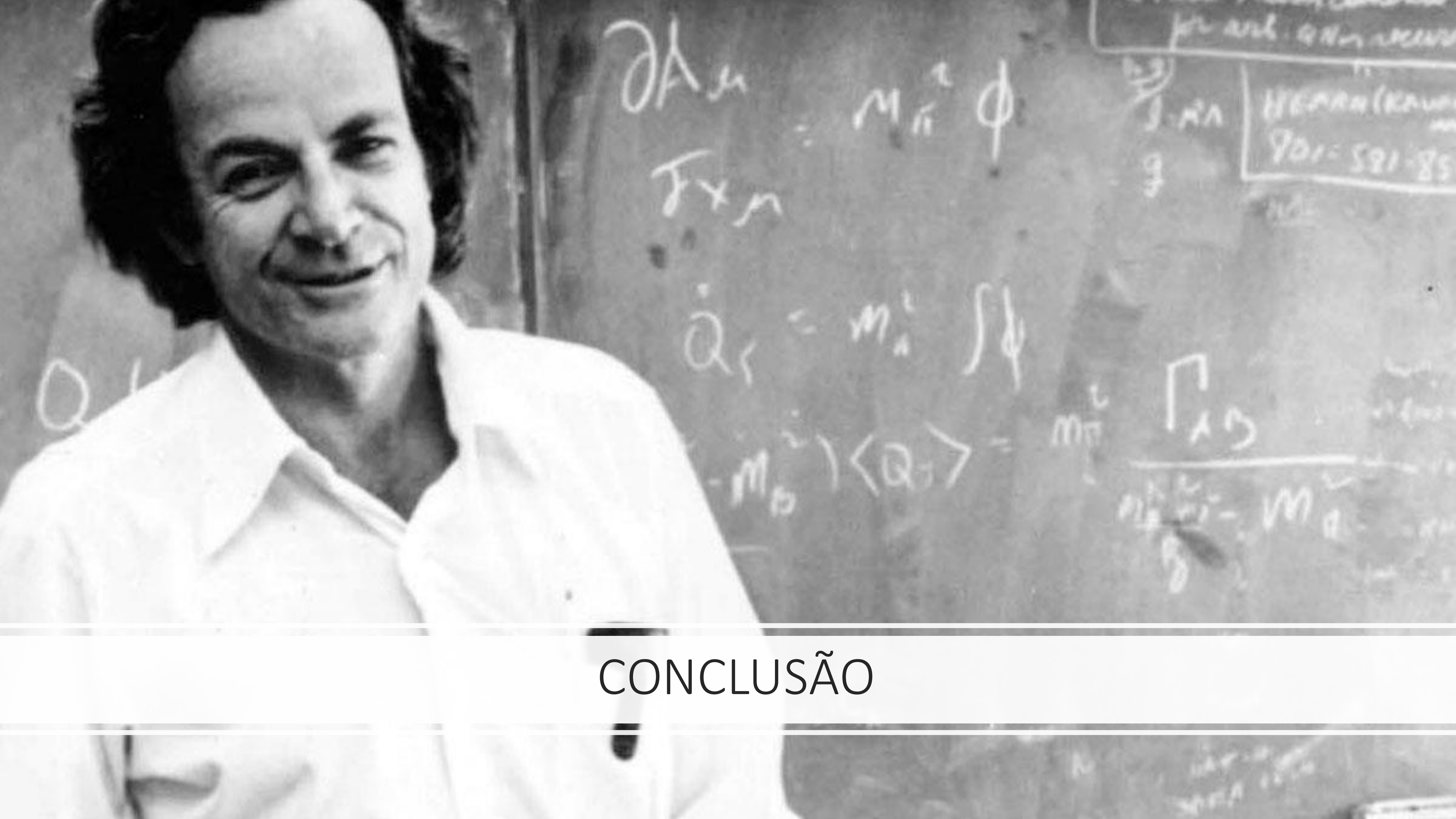
Projeto Open Source Brasileiro



Coordenador do Projeto Eduardo Maschio

https://www.linkedin.com/in/eduardomaschio/

doomsk888@gmail.com



CONCLUSÃO

Referências Bibliográficas

- [1] S. Akama, Elements of Quantum Computing. Springer, 2014.
- [2] P. Benioff, “The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines,” Journal of Statistical Physics, vol. 22, no. 5, pp. 563–591, 1980.
- [3] J. Singh and M. Singh, ”Evolution in Quantum Computing,” 2016 International Conference System Modeling & Advancement in Research Trends (SMART), Moradabad, 2016, pp. 267-270.
- [4] D. Deutsch and R. Penrose, ”Quantum theory, the Church–Turing principle and the universal quantum computer,” Proceedings of the Royal Society, Oxford, 1985, pp. 97–117. [Online].Disponível em: https://royalsocietypublishing.org/doi/pdf/10.1098/rspa.1985.0070. Acessado em: 30, Mar., 2020.

Referências Bibliográficas

- [7] S. S. Sysoev, ’The Characteristics of Computational Systems’, Saint Petersburg State University, 2014. [Online].Disponível em: https://www.coursera.org/learn/quantum-computing-algorithms. Acessado em: 7, Abr., 2020.
- [8] J. P. S. Francese. Criptografia Quantica, Universidade Federal do Rio do Janeiro, 2008[Online]. Disponível em: https://www.gta.ufrj.br/grad/08 1/quantica/cap2.html. [Acessado 24 Fev. 2020]
- [9] Medium. M. Gayatri, Quantum Computing Basics — A simple explanation, 2019[Online]. Disponível em: https://medium.com/discourse/quantum-computing-basics-a-simpleexplanation-44f122dc09fa.[Acessado 24 Fev. 2020]


Thank you!
grammarly

ConFLOSS

O que é Computação Quântica

- O que é Computação quântica?
- Conceitos básicos da Computação Quântica e diferenças com a computação clássica: como surgiu
- Experiência de Schrodinger(sem se aprofundar nos conceitos de mecânica quântica)
- Qubit vs Bit
- Porta lógica quântica vgs porta lógica clássica
- Linguagens, para o quê servem
- Caso especial da computação quântica: o algoritmo de Shor
- Trabalhos Open source que estão sendo desenvolvidos
- O que existe no mercado