Základy forenzních databází

Tereza Uhlíková

verze 2.0

Kdo jsem

Tereza Uhlíková

Ústav analytické chemie

skupina teoretické spektroskopie

místnost A277

https://web.vscht.cz/~uhlikovt/

tereza.uhlikova@vscht.cz

1. lekce

- Co je to databáze
- Proč, kdo, kdy, jak ...
- Něco málo z historie
- CAP problém

Dobrodružství kriminalistiky - televizní seriál
Dějiny psané Římem - Vojtěch Zamarovský

2. lekce

- Základy informatiky
- Software
  - informace
  - záznam informace
  - číselné soustavy
  - písmenné kódy
- Hardware
  - Alan Turing, John von Neumann a počítač
  - historie vývoje počítače & super počítač
  - procesor a datová uložiště
- Architektura databází

Alan Turing - Enigma
Contact film z roku 1997; seti@home

3. lekce

- Algoritmus
  - vlastnosti
  - zápis
  - struktura
- Datové typy

Arthur C. Clarke - Devět miliard božích jmen

4. lekce

- Výroková logika
- Databáze
  - DB a SŘBD
  - databázové modely
- Relační model
  - návrh tabulky

Aghata Christie - Hercules Poirot

5. lekce

- ERA model
- Klíče, integrita a kardinalita
- Normalizace databáze

6. lekce

- Datové struktury
- Ukládání
- Složitost
- Řazení
- Přenos dat

7. lekce

- Vyhledávání
  - sekvenční
  - binární
  - hashing
- Jak google pracuje
- Neuronové sítě a Strojové učení

Blade Runner 1982
Terminátor 1984

Co bude dnes

- Proč kvantové počítače
- Hardware
- Qbit
- Základní principy - superpozice, provázanost, interference
- Využití, užitečné algoritmy pro vyhledávání
- Problémy

Co je to kvantový počítač

Co je to kvantový počítač

- Kvantový počítač není superpočítač, který dokáže všechno dělat rychleji. Ale počítač pracující na jiném principu.
- Do kvantového stavu molekuly můžeme zaznamenat informaci.
- Kvantové vlastnosti částic jsou využity pro reprezentaci a strukturu dat a kvantové jevy pak slouží k výkonu operací s těmito daty.

Co je to kvantový počítač

- Kvantový počítač není superpočítač, který dokáže všechno dělat rychleji. Ale počítač pracující na jiném principu.
- Do kvantového stavu molekuly můžeme zaznamenat informaci.
- Kvantové vlastnosti částic jsou využity pro reprezentaci a strukturu dat a kvantové jevy pak slouží k výkonu operací s těmito daty.

Může být v mnoho stavech v jednom čase (superpozice, provázanost, interference).
x×
Klasický může být pouze v jednom stavu v jednom čase.

Kyber hrozby

Novinky.cz » Internet a PC » Bezpečnost » Takovým hrozbám jsme ještě nečelili, obávají se experti kvantových

Takovým hrozbám jsme ještě nečelili, obávají se experti kvantových PC

8. 8. 2023, 14:16
Ondřej Husák

Umělá inteligence, chemický průmysl, předpověď počasí či lékařský výzkum. Kvantové počítače slibují zásadní zlom v mnoha oblastech lidského bádání. Stejně tak ale přinesou kvantové výpočty úplně novou generaci bezpečnostních hrozeb. Upozornili na to experti z kyberbezpečnostní společnosti Check Point.

kyber hrozby

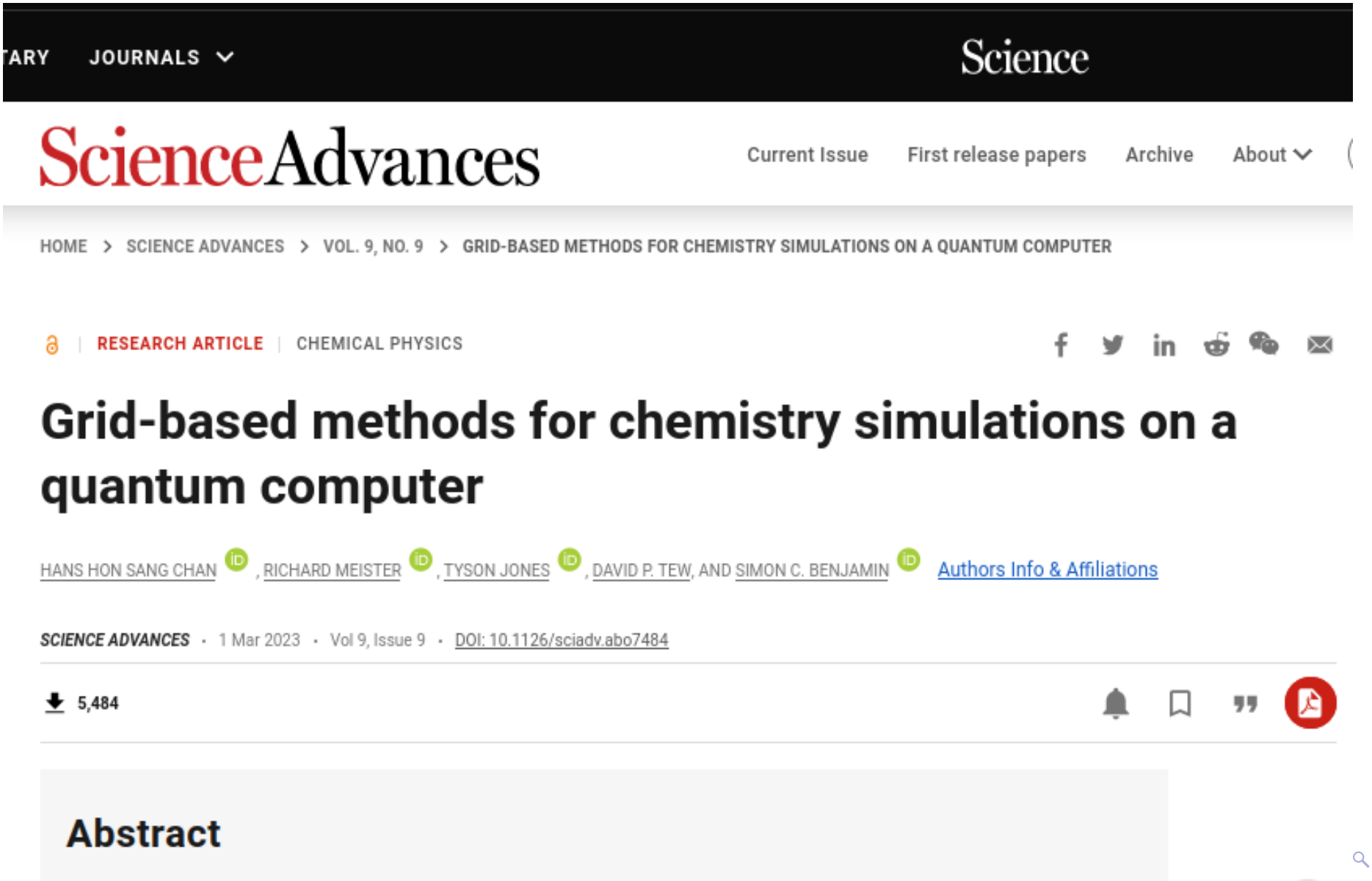
Kvantová nadřazenost

Home › Zprávičky

Google tvrdí, že jeho kvantový počítač dosáhl tzv. kvantové nadřazenosti

ČTK — 24. 10. 2019 | Zprávičky

Využití v chemii



TARY JOURNALS

Science

ScienceAdvances

Current Issue First release papers Archive About

HOME > SCIENCE ADVANCES > VOL. 9, NO. 9 > GRID-BASED METHODS FOR CHEMISTRY SIMULATIONS ON A QUANTUM COMPUTER

RESEARCH ARTICLE | CHEMICAL PHYSICS

Grid-based methods for chemistry simulations on a quantum computer

HANS HON SANG CHAN, RICHARD MEISTER, TYSON JONES, DAVID P. TEW, AND SIMON C. BENJAMIN Authors Info & Affiliations

SCIENCE ADVANCES · 1 Mar 2023 · Vol 9, Issue 9 · DOI: 10.1126/sciadv.abo7484

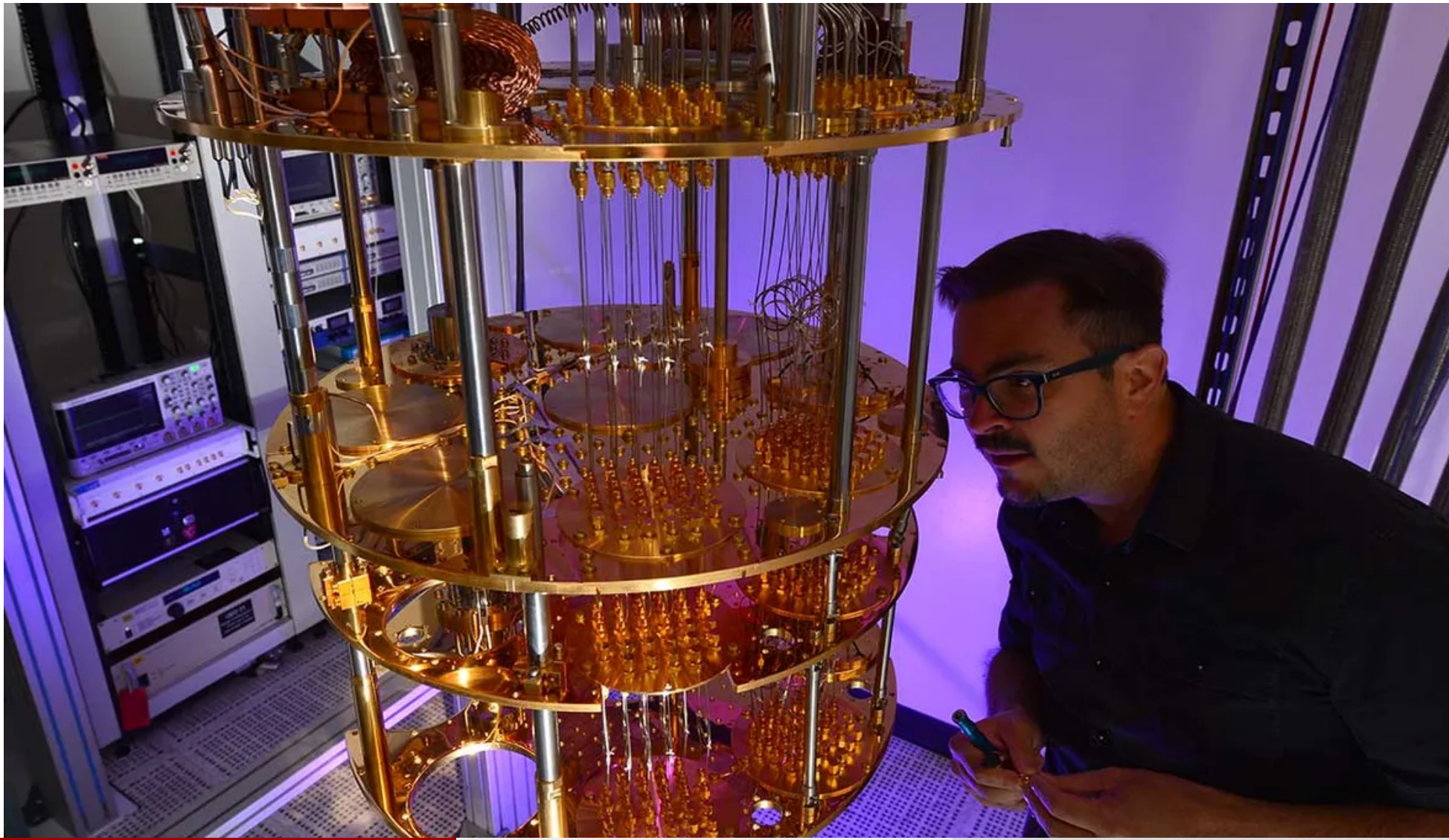
5,484

Abstract

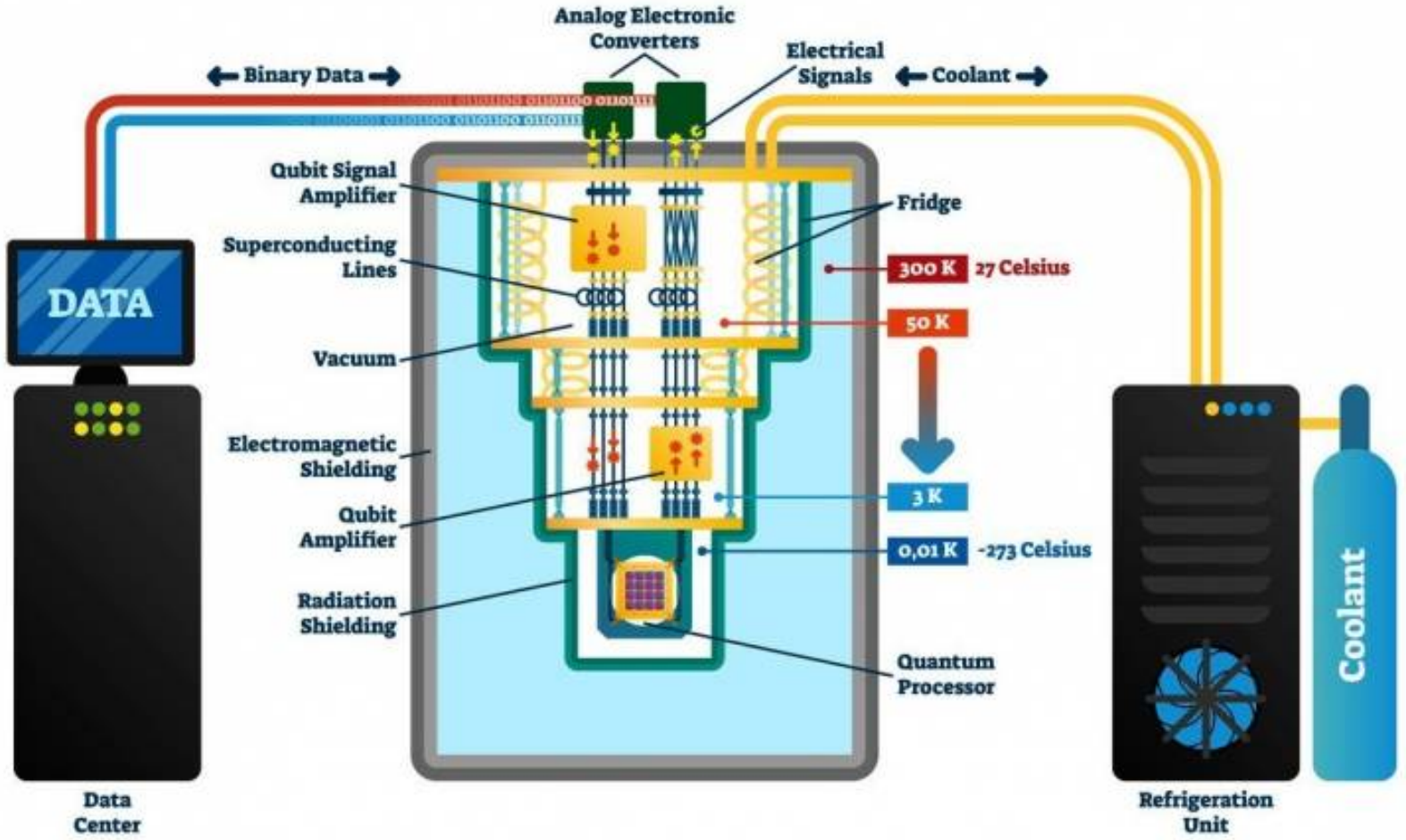
Hardware zvenku - stínění

Hardware - chlazení

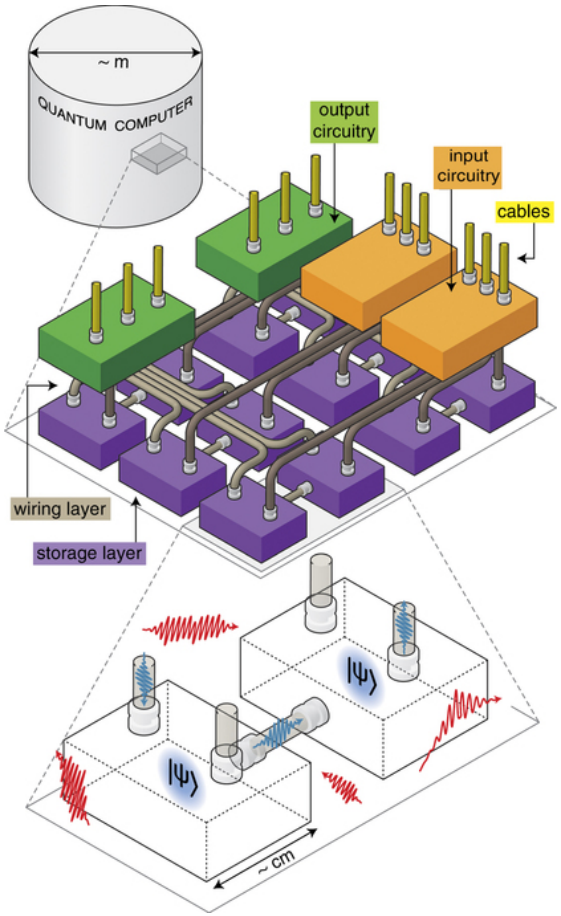
Hardware - bez chlazení



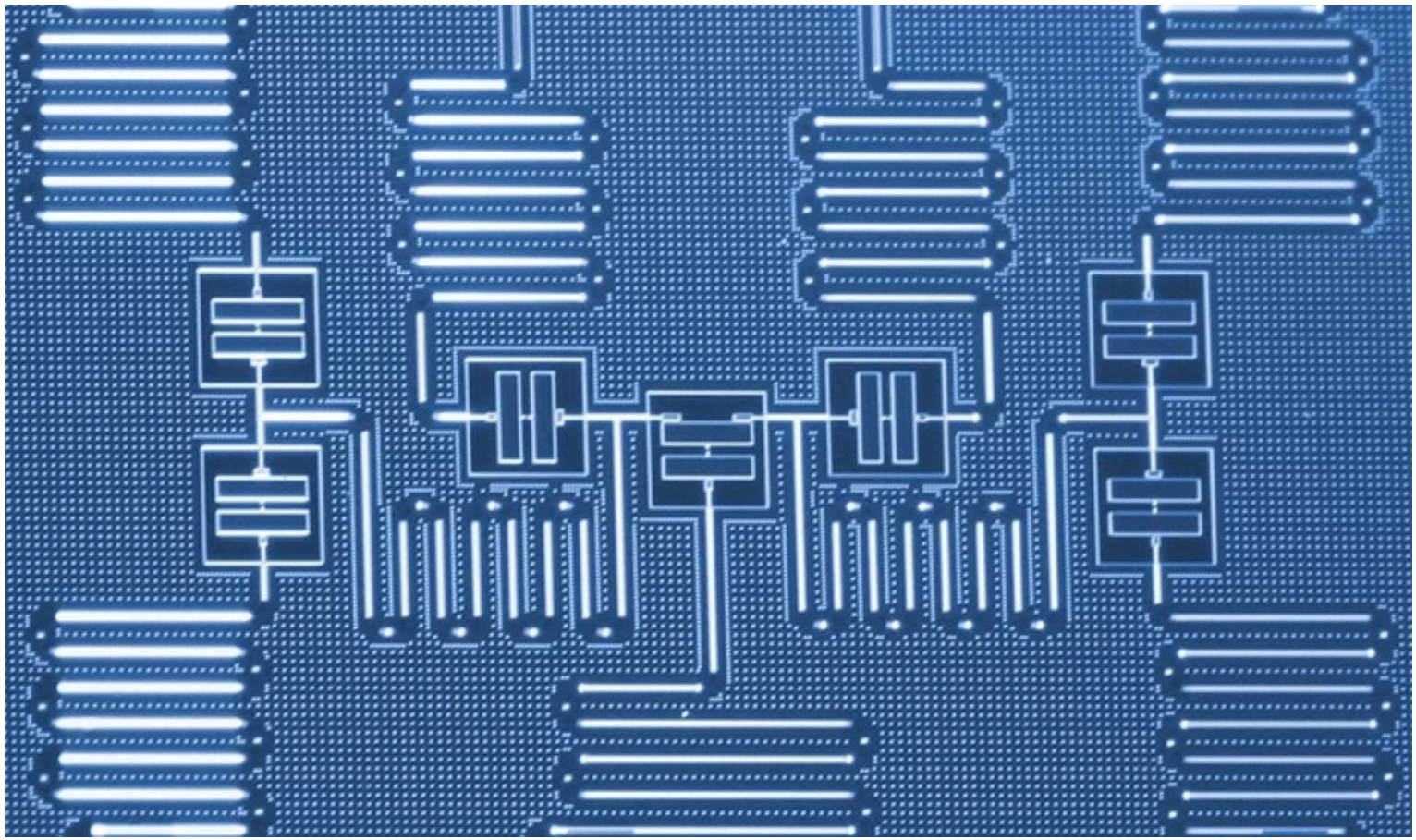
Hardware - náčrtek



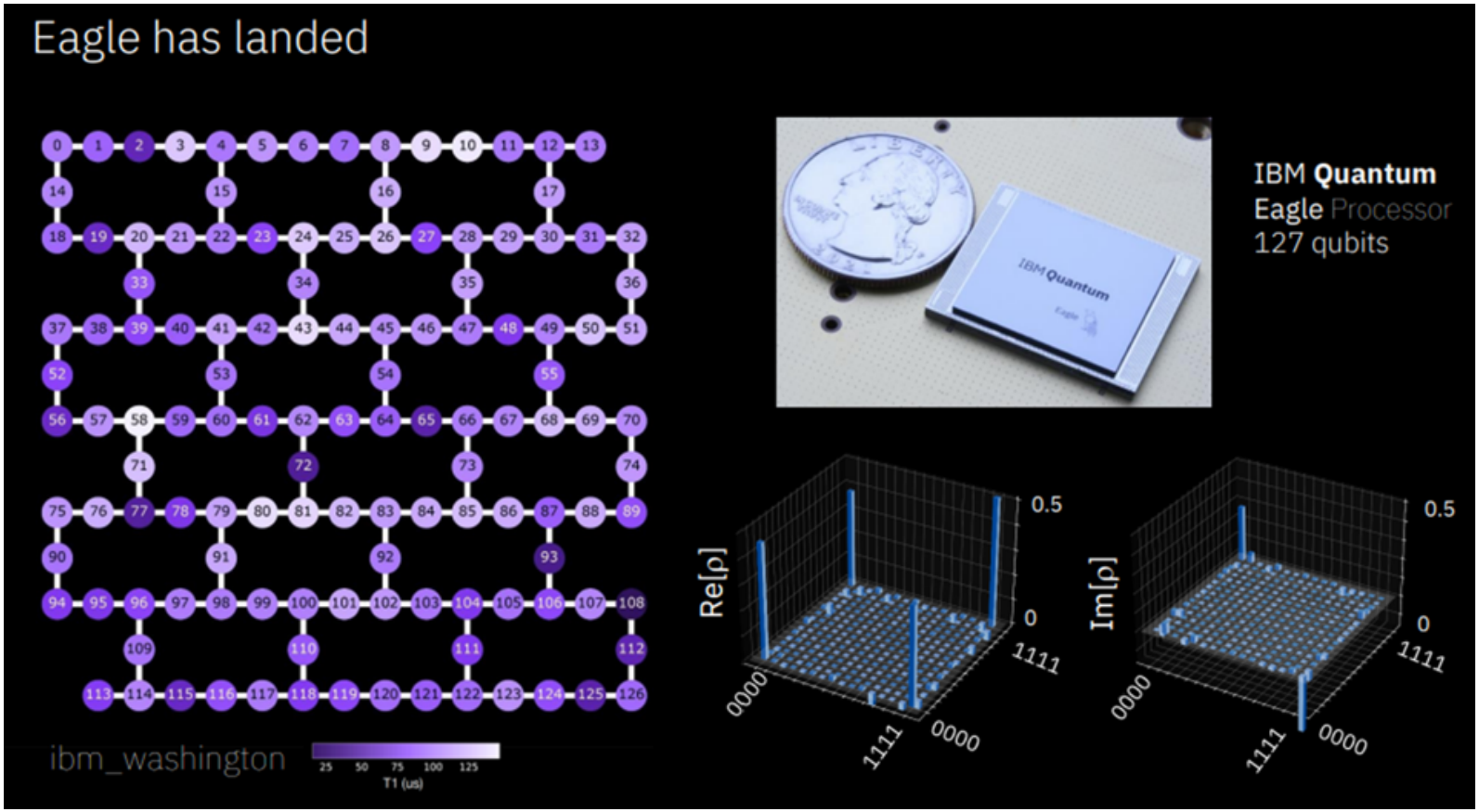
Hardware - náčrtek



Hardware - 7 qbitů



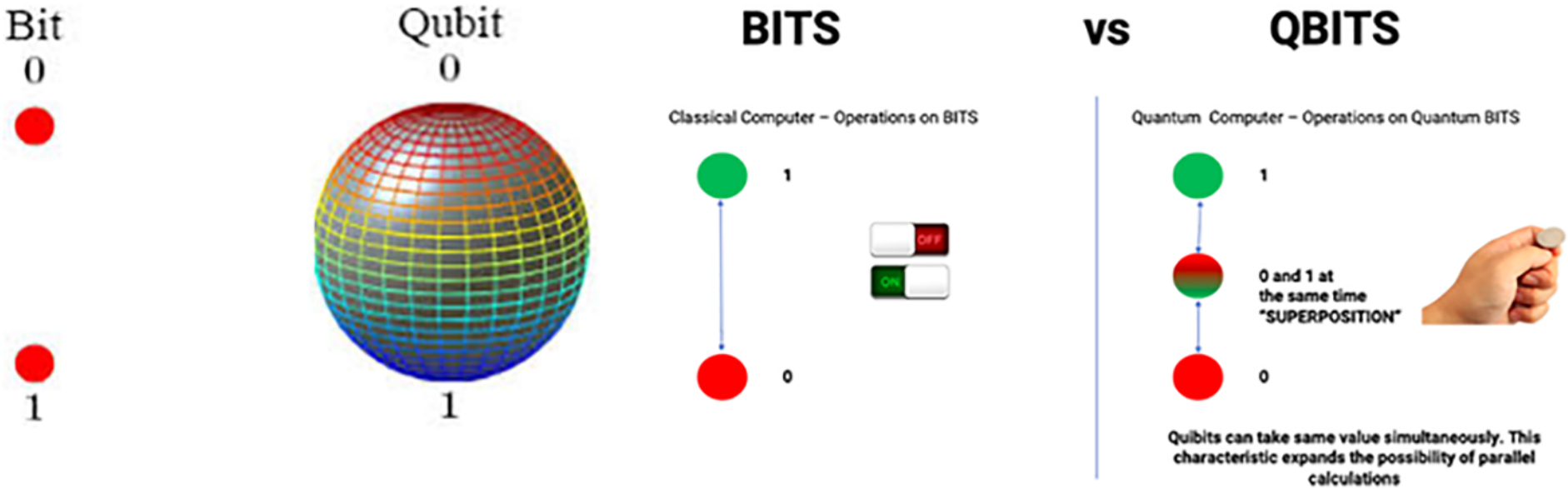
Hardware - 127 qbitů - IBM 2021



Hardware

https://www.newscientist.com/question/what-is-a-quantum-computer/

Bit x Qbit

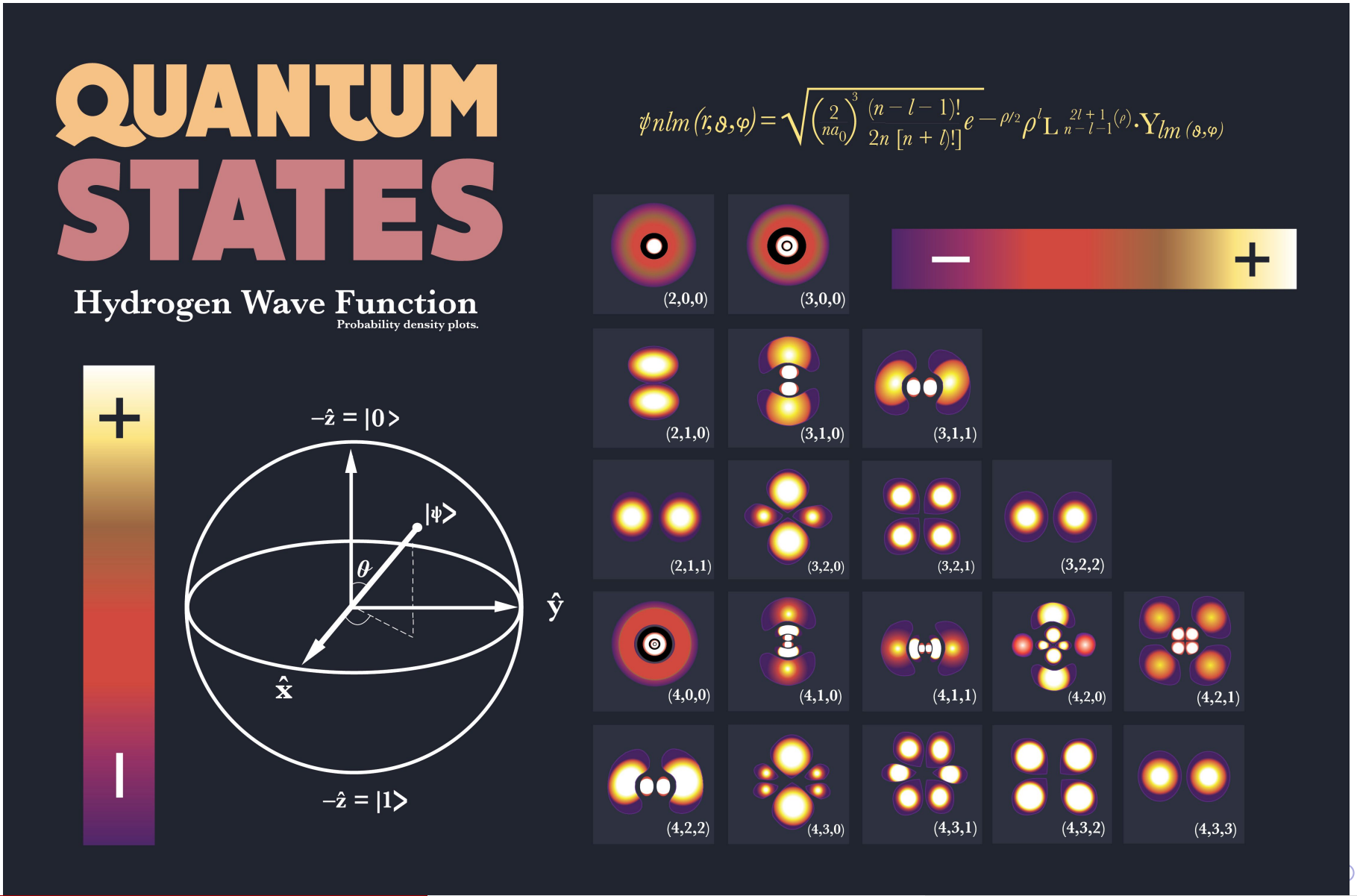

Bit
0
1
Qubit
0
1
BITS
vs
QBITS
Classical Computer – Operations on BITS
1
0
OFF
ON
Quantum Computer – Operations on Quantum BITS
1
0 and 1 at
the same time
"SUPERPOSITION"
0
Quibits can take same value simultaneously. This characteristic expands the possibility of parallel calculations

Tři věci

- superpozice (superposition)
- provázanost (entanglement)
- interference (interference)

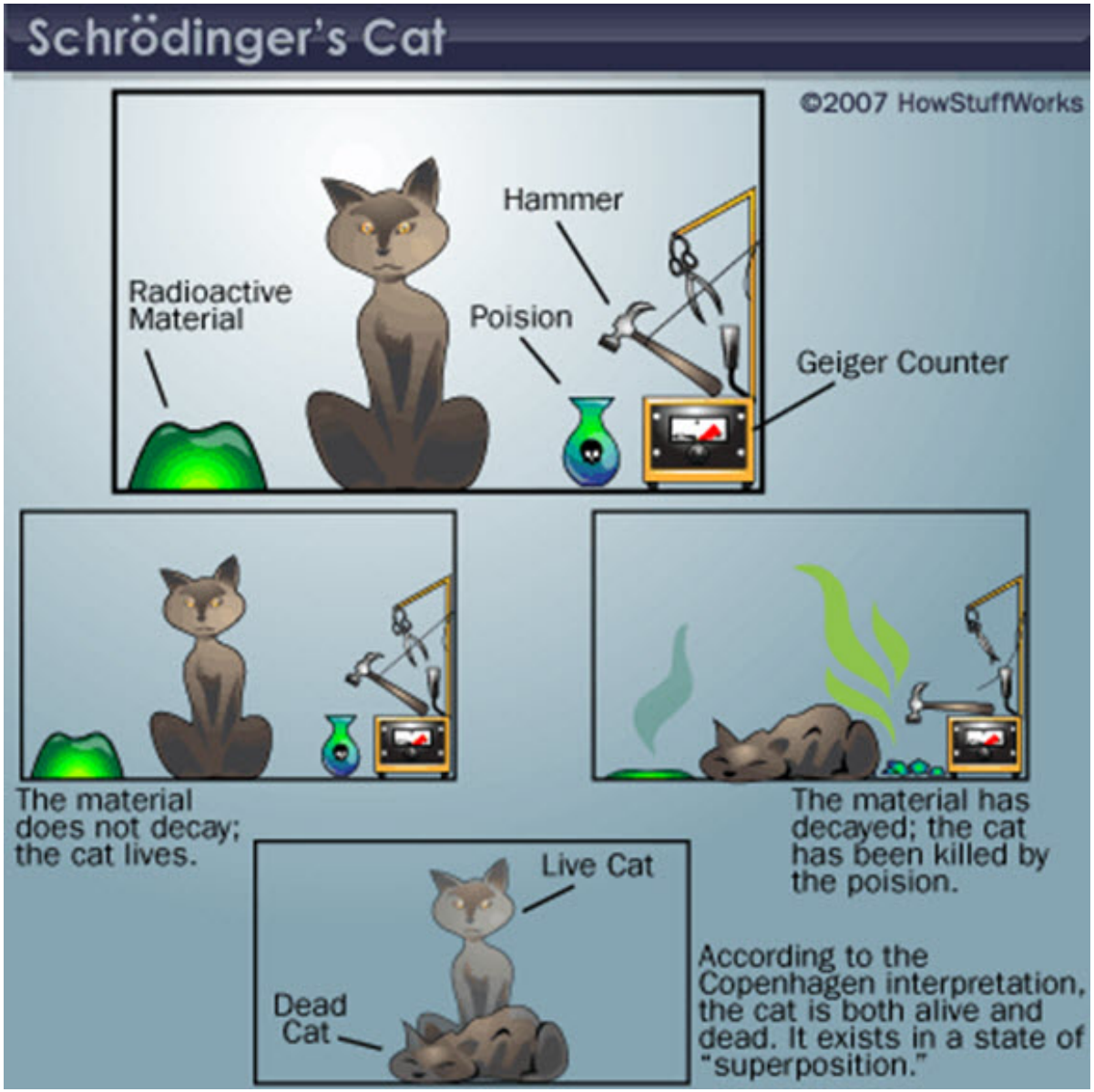
Stav

Stav

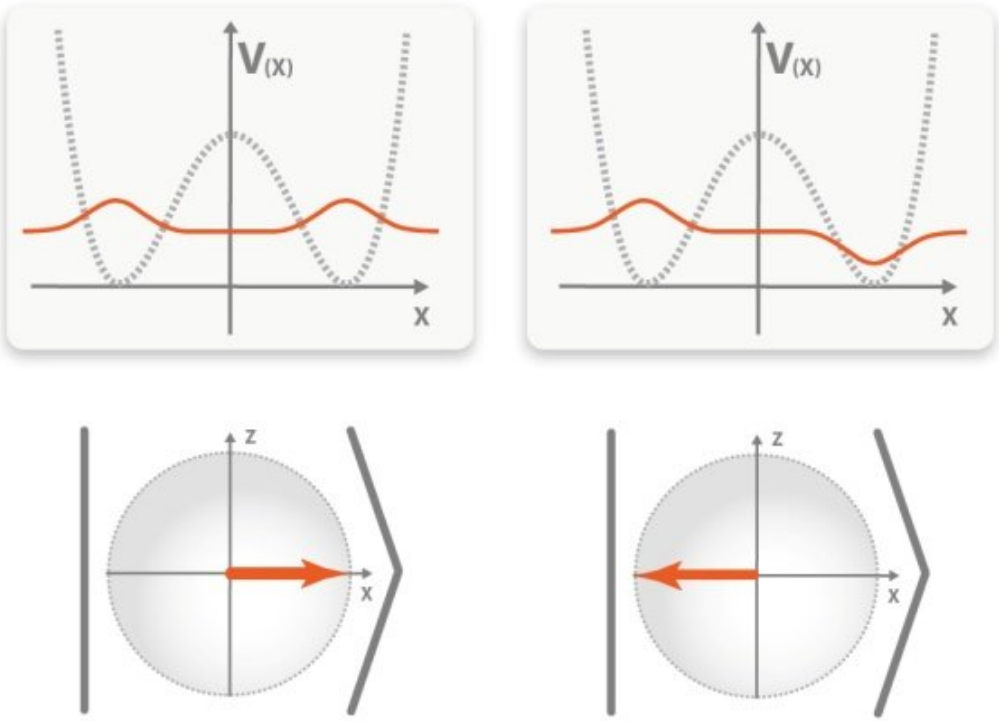

QUANTUM
STATES
Hydrogen Wave Function
Probability density plots.
$\psi nlm(r,\vartheta,\varphi) = \sqrt{\left(\frac{2}{na_0}\right)^3 \frac{(n-l-1)!}{2n\,[n+l)!]}} e^{-\rho/2} \rho^l L^{2l+1}_{n-l-1}(\rho) \cdot Y_{lm}(\vartheta,\varphi)$
(2,0,0)
(3,0,0)
(2,1,0)
(3,1,0)
(3,1,1)
(2,1,1)
(3,2,0)
(3,2,1)
(3,2,2)
(4,0,0)
(4,1,0)
(4,1,1)
(4,2,0)
(4,2,1)
(4,2,2)
(4,3,0)
(4,3,1)
(4,3,2)
(4,3,3)
+
|
$-\hat{z} = |0>$
$|\psi>$
θ
$\hat{y}$
$\hat{x}$
$-\hat{z} = |1>$

Schrödingerova kočka 1937

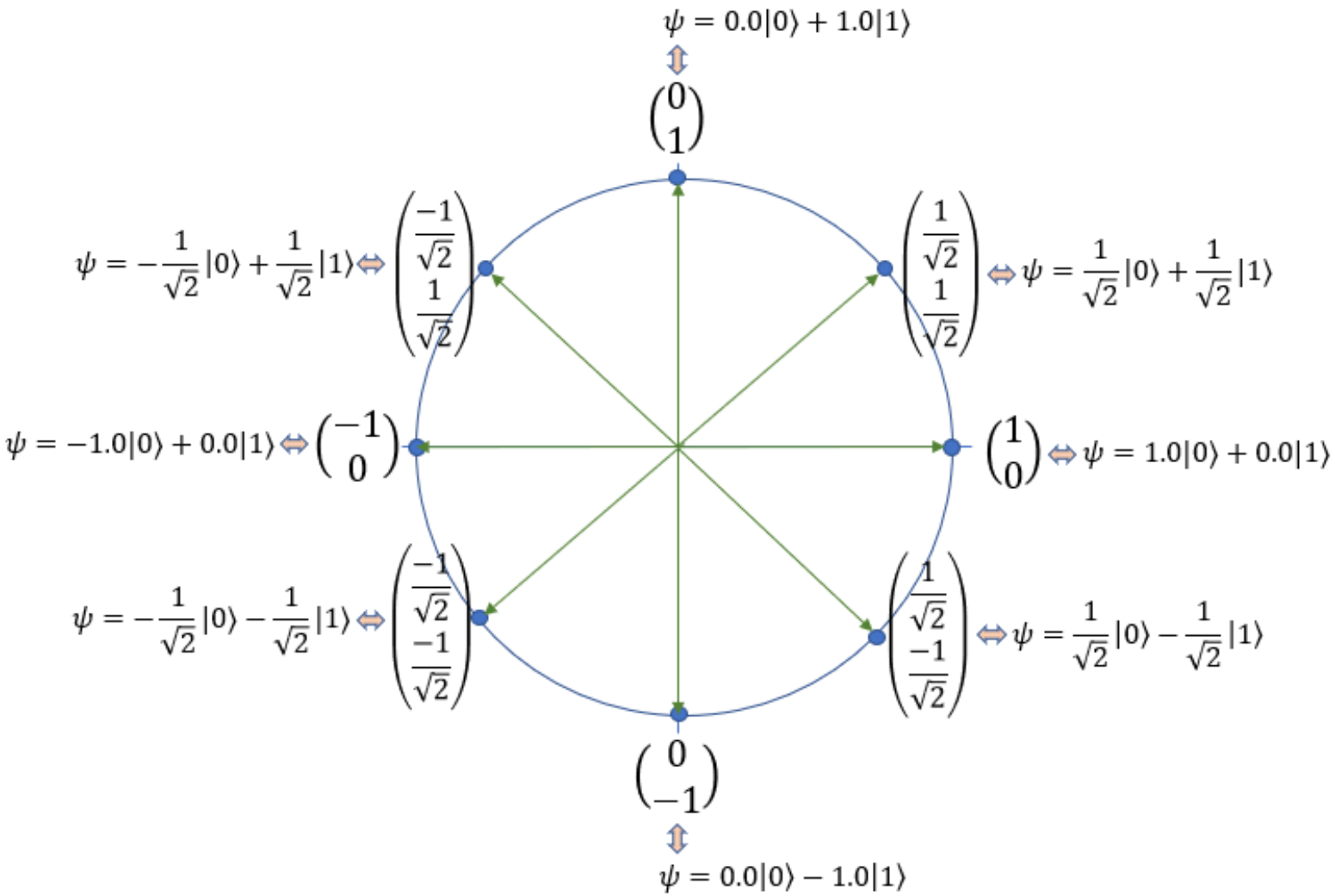
Schrödingerova kočka 1937



Superpozice



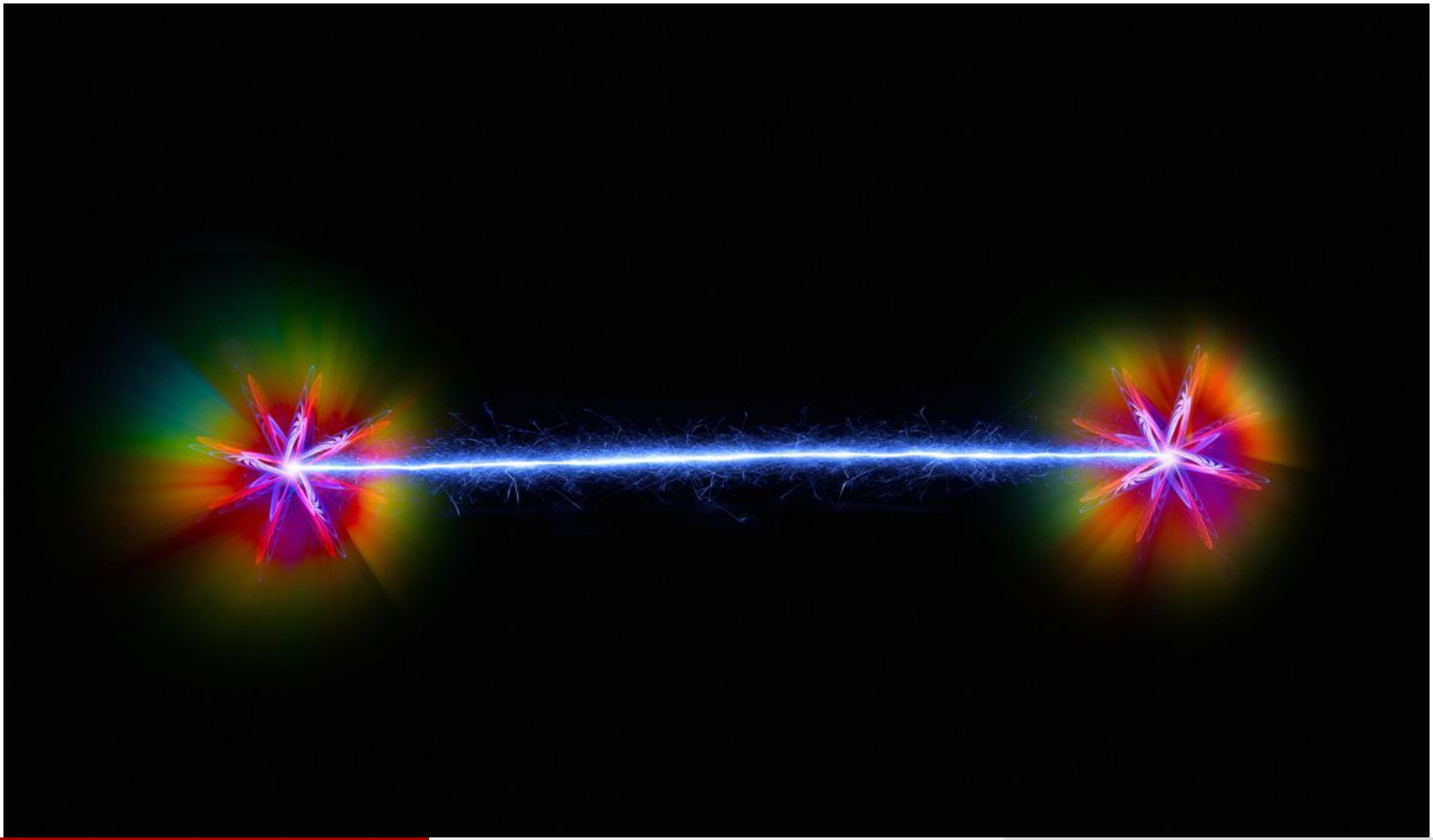
Qbit


$\psi = 0.0|0\rangle + 1.0|1\rangle$
$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$
$\psi = -\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \Leftrightarrow \begin{pmatrix} \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$
$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \Leftrightarrow \psi = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
$\psi = -1.0|0\rangle + 0.0|1\rangle \Leftrightarrow \begin{pmatrix} -1 \\ 0 \end{pmatrix}$
$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \Leftrightarrow \psi = 1.0|0\rangle + 0.0|1\rangle$
$\psi = -\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \Leftrightarrow \begin{pmatrix} \frac{-1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix}$
$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix} \Leftrightarrow \psi = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$
$\begin{pmatrix} 0 \\ -1 \end{pmatrix}$
$\psi = 0.0|0\rangle - 1.0|1\rangle$

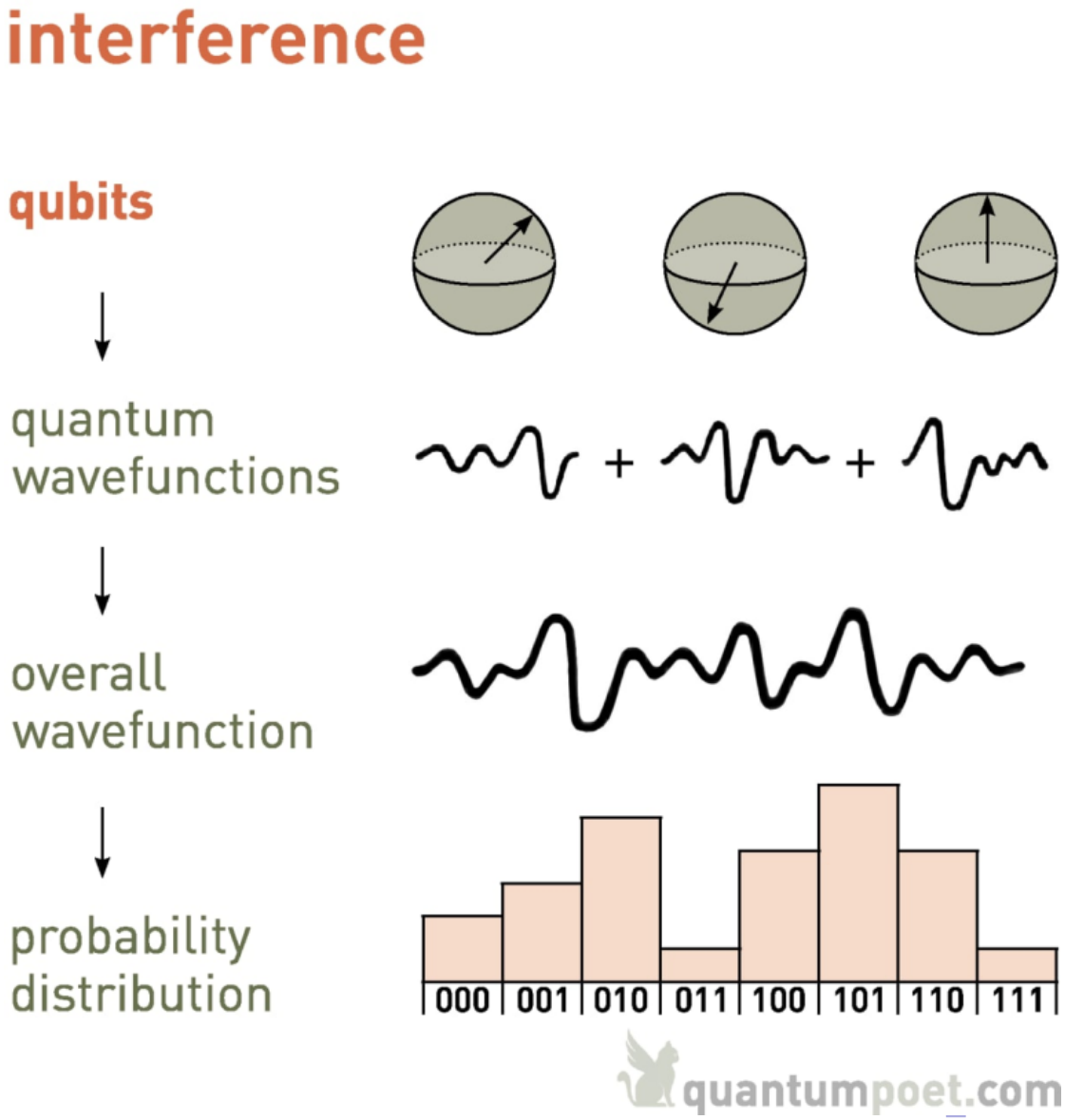
Provázanost

2022 - nobelova cena - Alain Aspect, John F. Clauser, and Anton Zeilinger

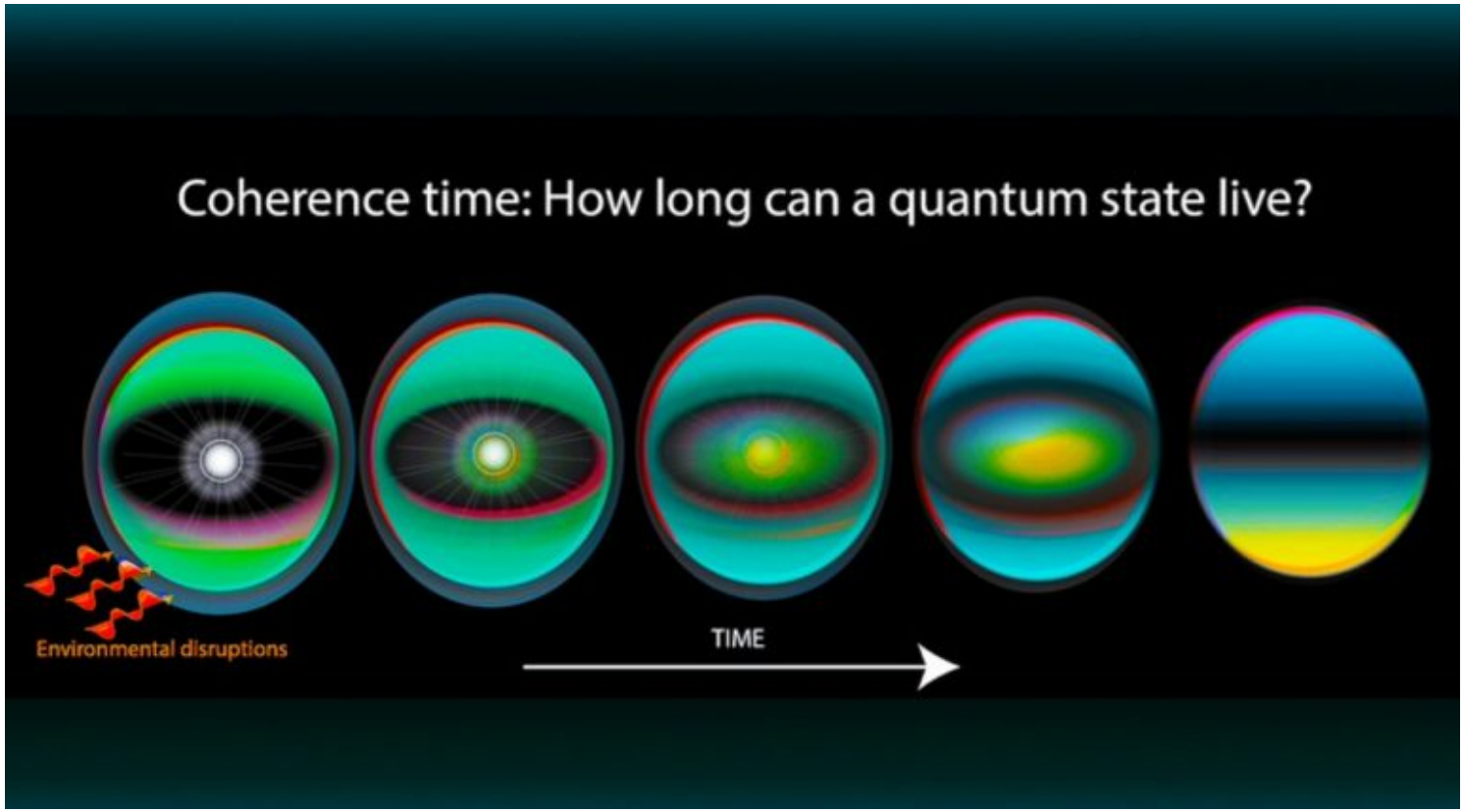
$$|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_A \otimes |H\rangle_B - |V\rangle_A \otimes |V\rangle_B\right)$$



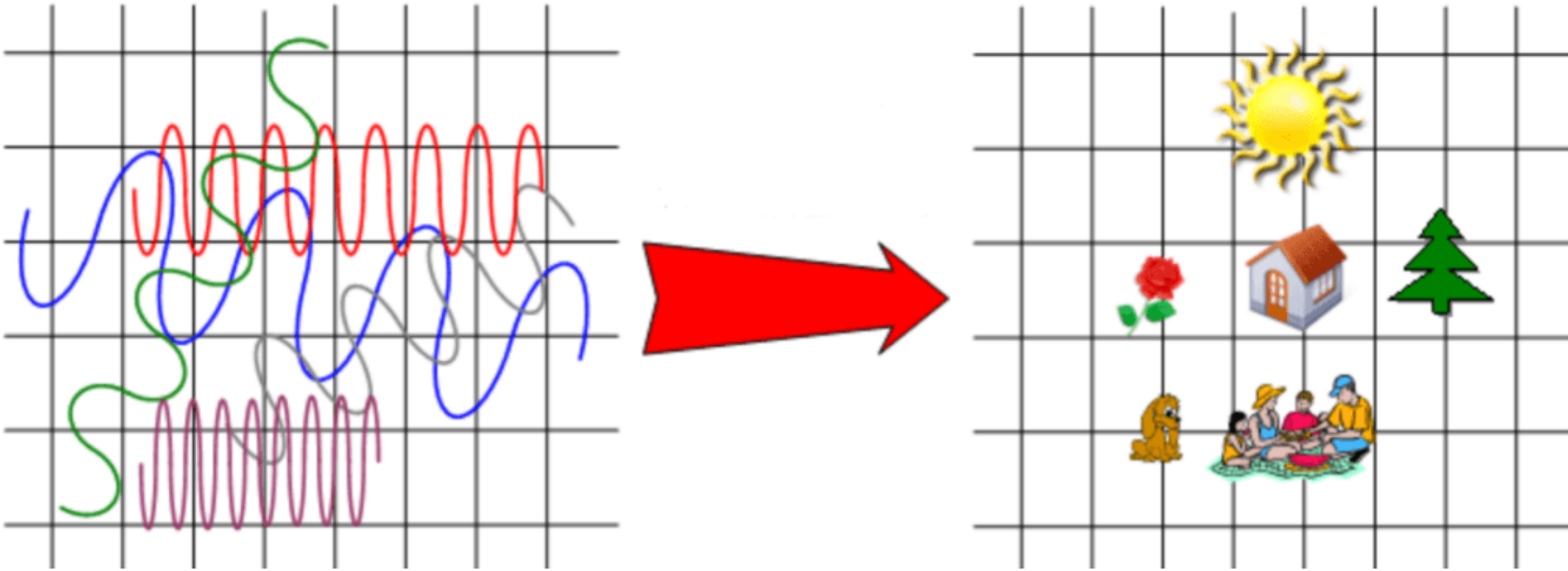
interference



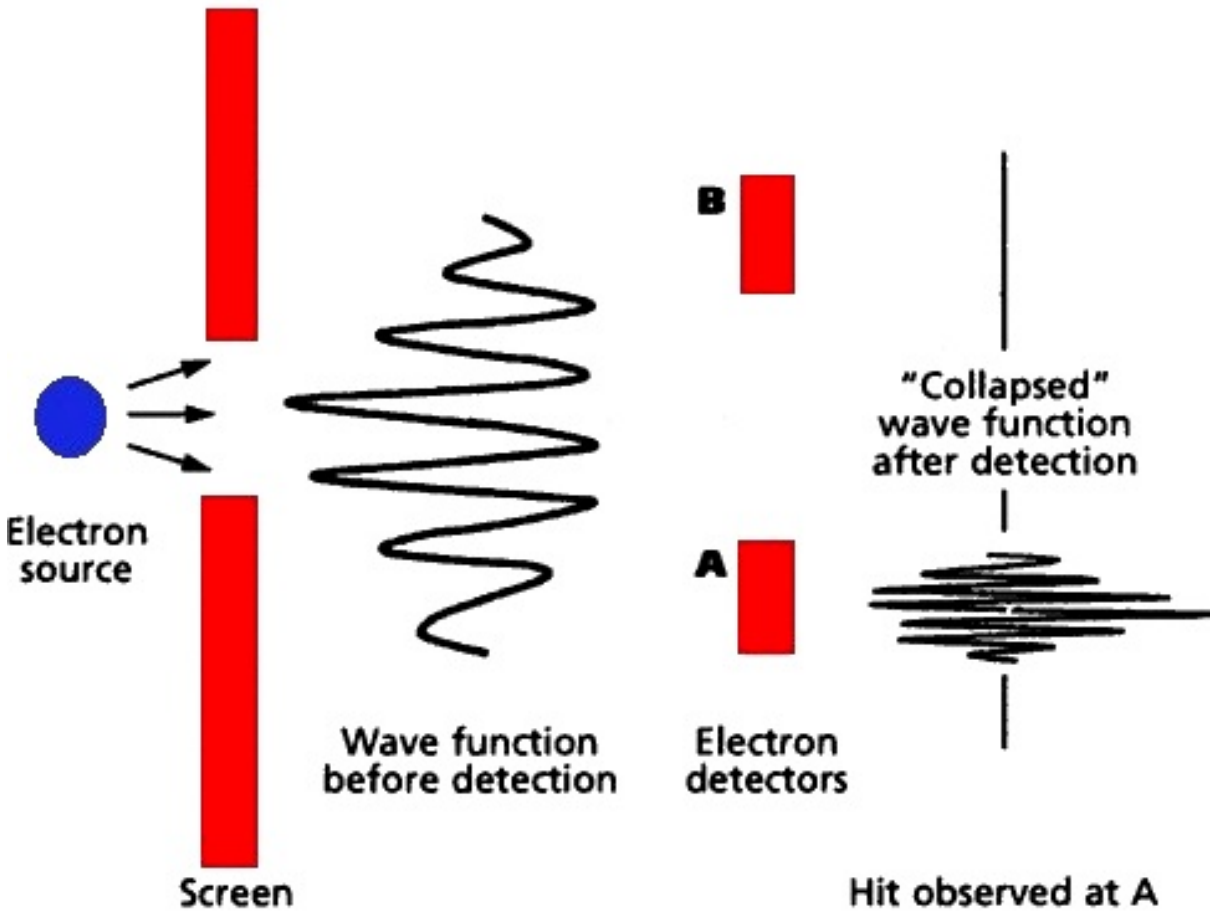
Evoluce stavu



Kolaps při pozorování



Kolaps při pozorování



Qbit

QUBIT A JEHO VYUŽITÍ

GRAFICKÝ MODEL QUBITU V PODOBĚ BLOCHOVY SFÉRY.

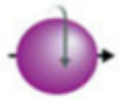
Souřadnice
N 23°34´41,4422˝;
E 32°48´10,3476˝,
znázorněné kruhy
vyjadřují superpozici
pravděpodobnosti stavů
(70 % pro spin nahoru,
30 % pro spin dolů)

LOGICKÉ HODNOTY QUBITŮ

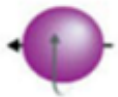
0 Spin dolů

1 Spin nahoru

|0> Superpozice blíže 0

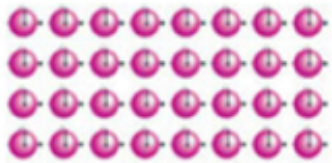


|1> Superpozice blíže 1

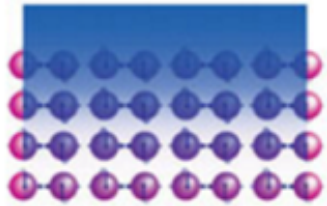


PRINCIP KVANTOVÝCH VÝPOČTŮ

1. Před začátkem výpočtu



2. Částice jsou vystaveny laseru

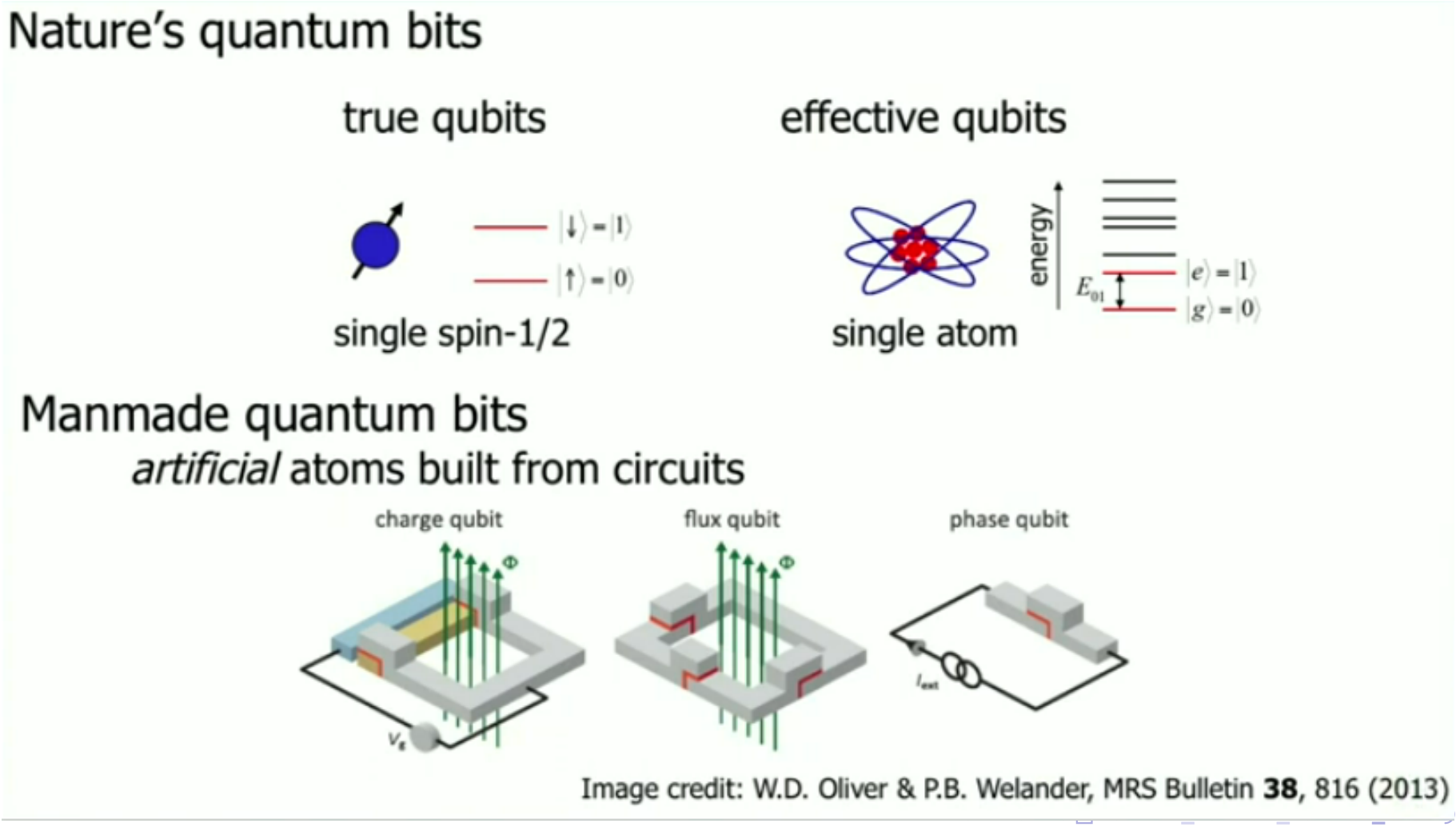


3. Výsledek

Fyzický qbit

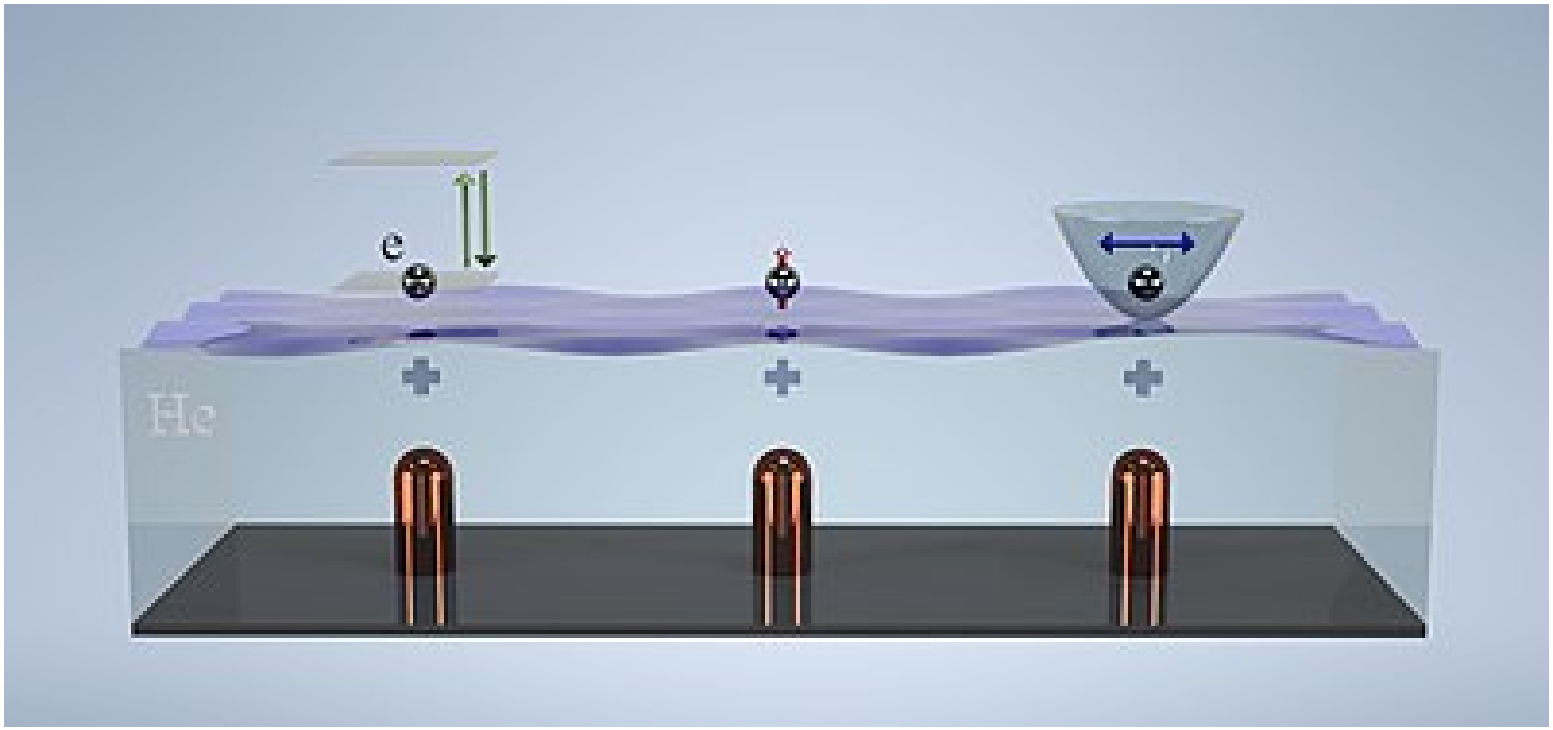
https://en.wikipedia.org/wiki/List_of_proposed_quantum_registers

transmon



Fyzický qbit

Iontové pasti
NMR - využívá spinu
Vibrační - superpozice vibračních stavů
Fullerenové ($N@C_{60}$)
Electron-na-heliu



video

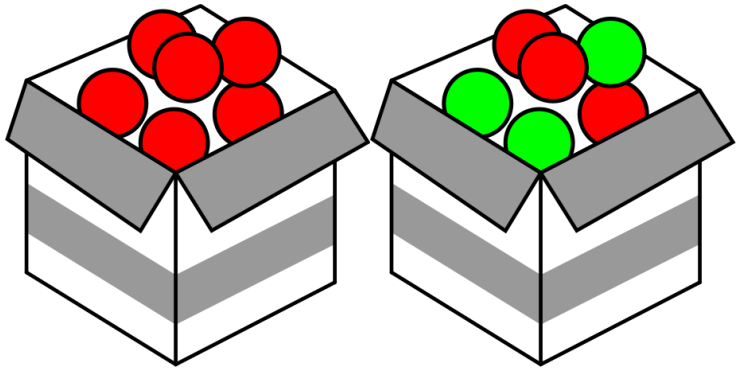
https://www.aldebaran.cz/bulletin/2017_37_kvp.php

Jak programovat Qbity

Úkol: Hledání osoby. Všichni víte svoje jméno (stav qbitu). Všichni víte zároveň o všech ostatních (provázanost). Zeptám-li se na konkrétní jméno, okamžitě dostanu výsledek na jeden průchod.
Karty
Bludiště

Deutsch - Jozsa algoritmus

1992 David Deutsch a Richard Jozsa



Máme funkci (černou krabičku) $f : 0,1^n \rightarrow 0,1$
je buď konstanta (stejný výstup pro všechna x)
nebo balancovaná (rovná se 0 nebo 1 přesně v polovině případů x).
Jak zjistit, jestli je funkce konstanta nebo balancovaná?
Klasický počítač: složitost $O(2^N)$
Kvantový počítač: 1 průchod

Shorův algoritmus

RSA šifrování
obecně známá faktorizace čísla
$3 \cdot 5 = 15$
$437 = 19 \cdot 23$
Klasický počítač: $O(\exp b)$

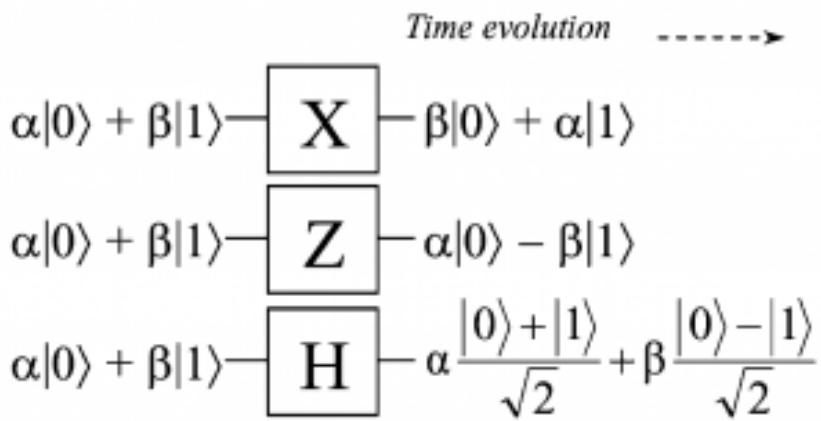
1994 Peter Shor
Faktorizace čísla na základě zkoumání posloupnosti číslic a zjišťování jejich periodičnosti
Kvantový počítač: Složitost polynom $O(b^3)$

Groverův prohledávací algoritmus

1996 Lov Grover
Klasický počítač: $O(N)$
Kvantový počítač: $O(\sqrt{N})$
Obecně - Když částice, kvantový balíček potencionalit, narazí do bariéry nebo je jinak vyrušena, záporné vlnky se zkombinují s kladnými a v sebedestrukci zanechávají jen jedinou vlnku popisující možnost, která se realizuje v pozorovaném světě - kolabs vlnové funkce.
Nejprve jsou všechny položky převedeny na jedničky a nuly a společně umístěny v kvantové superpozici - inicializace qbitu.
Výsledkem je svazek vln reprezentujících jednotlivé položky. Pak systém ovlivněte - laserový impuls - tak, aby se vlnky pozitivních amplitud vyrušily s vlnkami negativních amplitud - vývoj systému v čase. Nakonec zbude jen vlnka reprezentující hledanou položku databáze - kolabs interferentní vlnové funkce do výsledku.

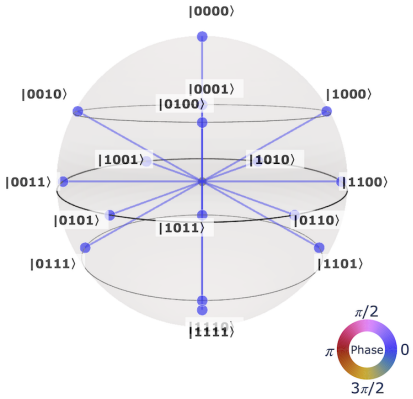
Jak programovat Qbity

fyzicky - mikrovlny, laserovým pulzem, magnetickým polem
informaticky - logické funkce nazvaná hradla
na 1 qbit:
Pauliho-X hradlo - přetáčí stav qubitu z $|0\rangle$ na $|1\rangle$ a $|1\rangle$ na $|0\rangle$ (ekvivalent funkce NOT u klasických bitů)
Pauliho-Z hradlo - ponechává $|0\rangle$ a přetáčí stav qubitu $|1\rangle$ na $-|1\rangle$ (přehození fáze)
Hadamardovo hradlo – snižuje pravděpodobnosti stavu qubitu $|0\rangle$ nebo $|1\rangle$ na polovinu

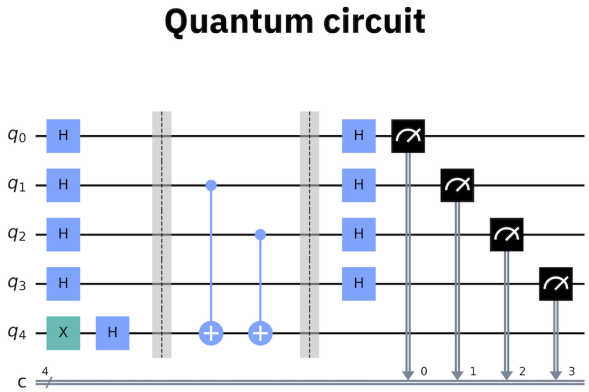


Quantum single qubit gates.

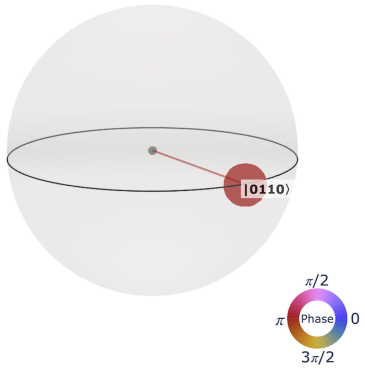
Operace s Qbity



Superposition of all possibilities



Computation driven interference



Solution

IBM Quantum experience

https://www.ibm.com/quantum/qiskit-runtime

Historie

1960 Stephen Wiesner - kvantové stavy jako nositele informace

1976 Roman Stanisław Ingarden - Quantum Information Theory

1980 Paul Benioff popíše počítač pomocí kvantové mechaniky

1982 Richard Feynman - navrhl použití kvantových systémů k výpočtům

1984 Charles Bennett a Gilles Brassard - kv. kryptografický protokol BB84

1985 David Deutsch - kvantový Turingův stroj

1994 Peter Shor - faktorizační algoritmus

1995 poslána zpráva kvantovým kanálem

1996 Lov Grover - vyhledávací algoritmus

1996 Peter Shor a Andrew Steane - kvantová oprava chyb možná

1997 uskutečněna kvantová teleportace

1999 Richard Huges - iontové pasti s desítkami qubitů

Historie

- 2001 IBM a Stanford University odzkoušeli Shorův algoritmus (číslo 15 na 7-qbitech)
- 2010 D-Wave One: první komenrční kvantový počítač (annealer)
- 2016 IBM - experience pro každého
- 2019 Google tvrdí kvantovou nadřazenost
- 2023 Česká republika bude hostit evropský kvantový počítač LUMI-Q
- 2024 IBM více jak 1000 qb

Problémy

dekoherence kvantových stavů
pohyb všeho - $T = 0\text{K}$
dokonalé stínění

Kvantová nadřazenost ?

ITARY JOURNALS Science

News Home All News ScienceInsider News Features

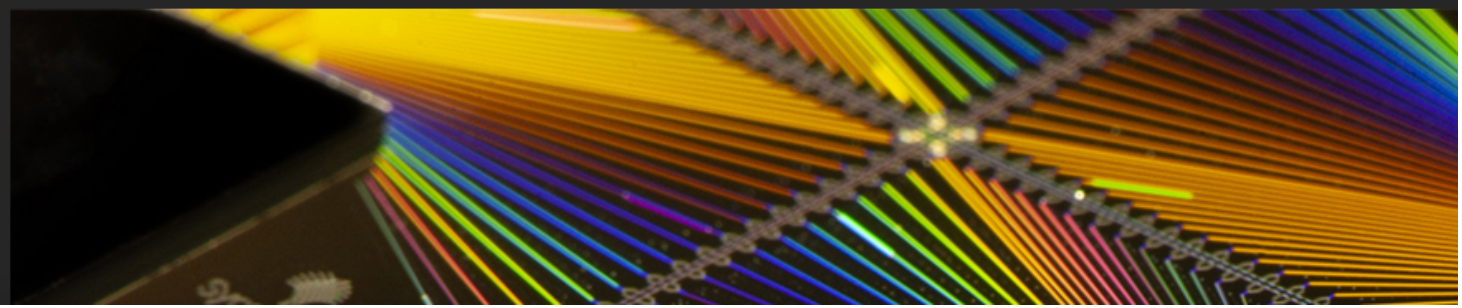
HOME > NEWS > ALL NEWS > ORDINARY COMPUTERS CAN BEAT GOOGLE'S QUANTUM COMPUTER AFTER ALL

NEWS | PHYSICS

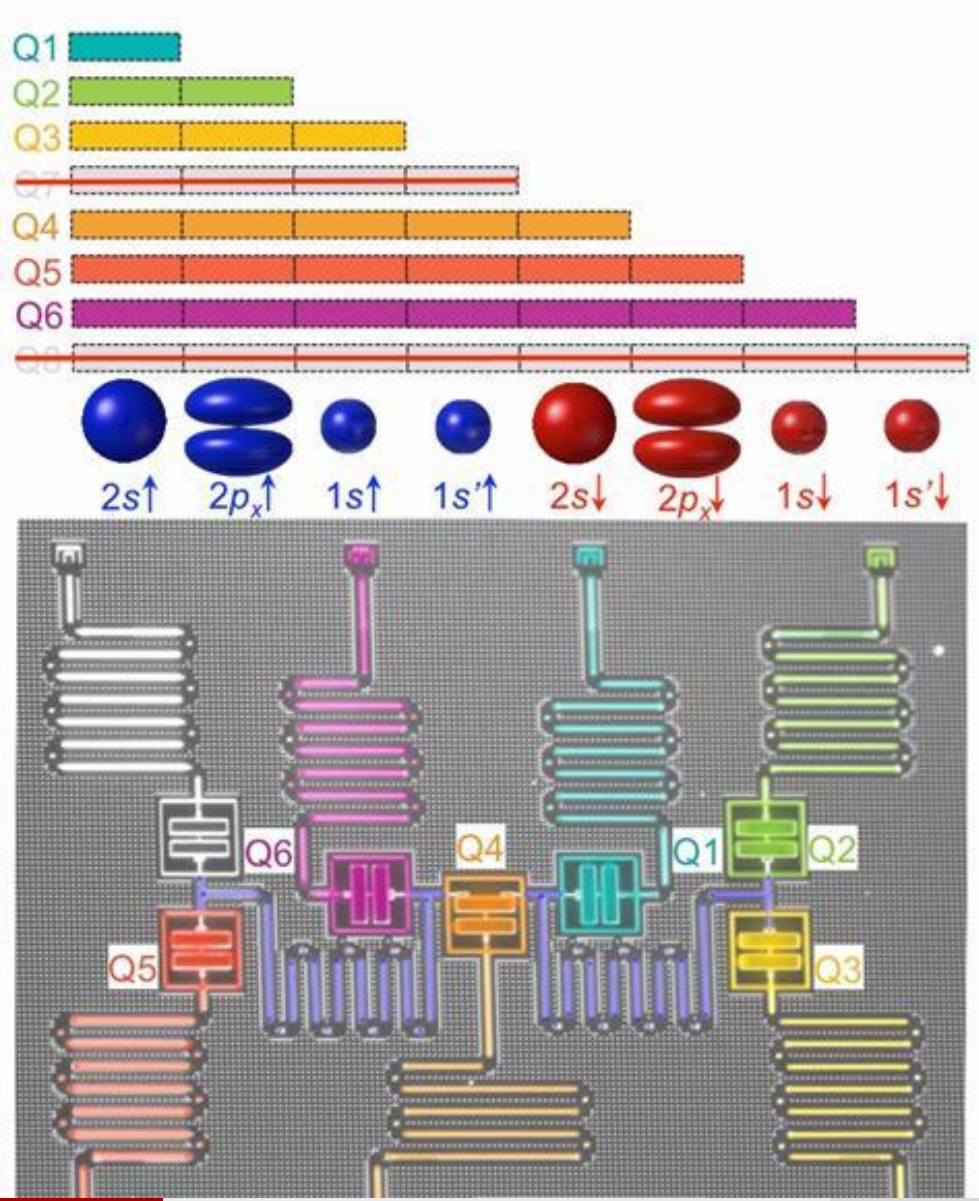
Ordinary computers can beat Google's quantum computer after all

Superfast algorithm put crimp in 2019 claim that Google's machine had achieved "quantum supremacy"

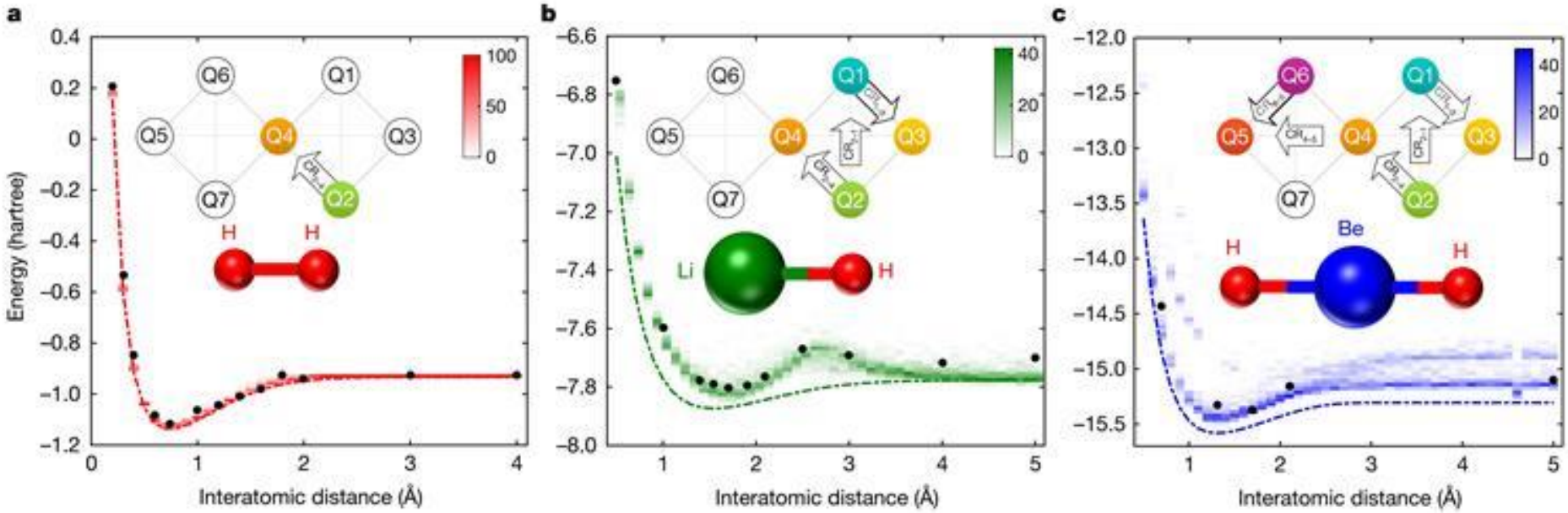
2 AUG 2022 · 5:05 PM ET · BY ADRIAN CHO



Využití v chemii



Využití v chemii



Co bude předmětem

1	18.9.	Úvod do databází, jejich účel a historie
2	25.9.	Architektura databází a informatika
3	2.10.	Programování - algoritmus, kódy, výroková logika
4	9.10.	Základy databází, klíče a kardinalita
5	16.10.	ERA model, normalizace
6	23.10.	Ukládání dat
7	30.10.	Vyhledávání
8	6.11.	Kvantové počítače pro práci s daty
9	13.11.	SQL + porovnání používaných (MySQL, SQL Server, MS Acce
10	20.11.	Návrh relační databáze I + cvičení v BS2 od 8:10
11	27.11.	Návrh relační databáze I + cvičení v BS2 od 8:10
12	4.12.	Opakování
13	11.12.	Zkouška
14	18.12.	Zkouška

Skripta, stránky a materiály

https://www.nukib.cz/download/publikace/podpurne_materialy/Utoky%20s%20vyuzitim%
https://www.karlin.mff.cuni.cz/~holub/soubory/qc/node24.html
https://spectrum.ieee.org/intels-quantum-computing-plans-hot-qubits-cold-control-chips-and-rapid-testing
https://learn.microsoft.com/cs-cz/azure/quantum/overview-algebra-for-quantum-computing
bakalařská práce groveruv algoritmus
https://dspace.cuni.cz/handle/20.500.11956/10944?show=full
https://www.chemistryworld.com/news/quantum-computer-tackles-its-first-triatomic/3007979.article
https://www.thebroadcastbridge.com/content/entry/14159/instant-answers-from-the-universe
https://development.ie/2021/12/the-basics-of-quantum-computing-quantum-superposition/
https://www.popularmechanics.com/science/a41521357/nobel-prize-in-physics-2022-quantum-entanglement/
https://quantumpoet.com/quantum-computing-introduction/
http://www.mysearch.org.uk/website1/html/549.Collapse.html
https://tanishabassan.medium.com/decoherence-quantum-computers-greatest-obstacle-67c74ae962b6