

Quantum Computers: What Are They Good For?

Rubem Mondaini

June 11th, 2024





ANNALS OF TECHNOLOGY

THE WORLD-CHANGING



FORBES > INNOVATION

Four Ways Quantum Computing Could Change

Forbes Councils Member
Technology Council
Membership (Fee-Based)

Jul 30, 2021, 07:20am EDT

[Back to McKinsey Themes](#)

How quantum computing could change the world



FT Podcast Tech Tonic [+ Add to myFT](#)

The quantum revolution: The way the world is

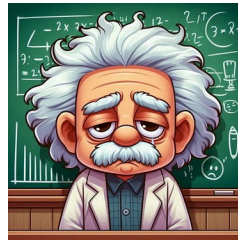
What quantum technology tells us about the true nature of reality

Quantum superposition and measurement



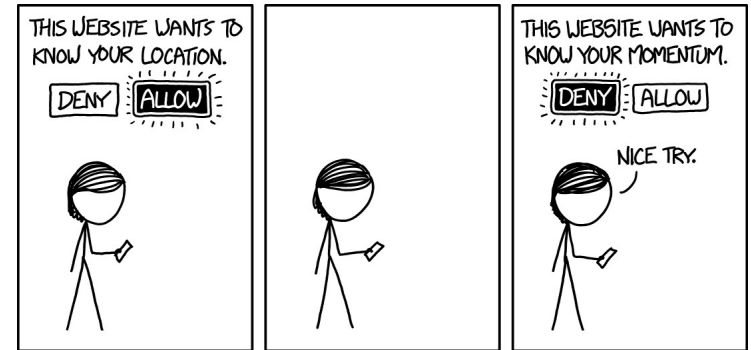
How these seemingly odd concepts can be used to perform quantum computations?

Quantum entanglement



(also known as "spooky action at distance" ...)

Quantum uncertainty principle



$$\Delta x \Delta p \geq \hbar/2$$

Computations

Classical
and
Quantum

Let's recall classical computation

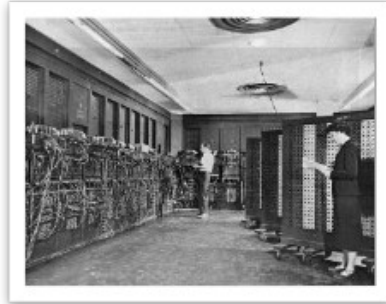
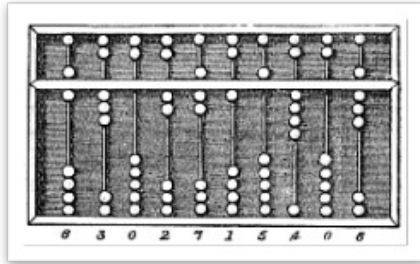
classical bit

data units:

'0' '1'

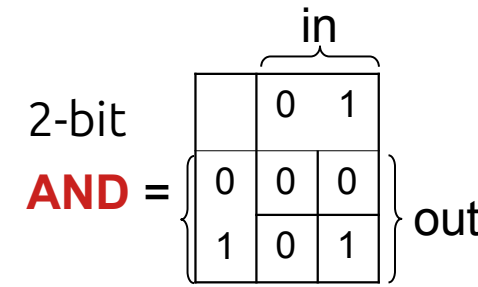
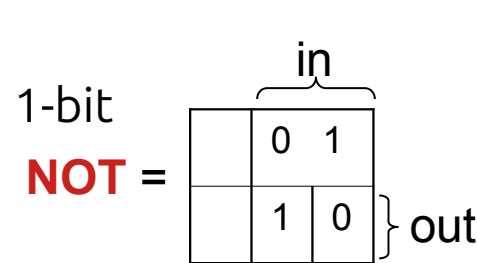
valid states:

$x = '0' \text{ or } '1'$



operations:

logical



Quantum computation



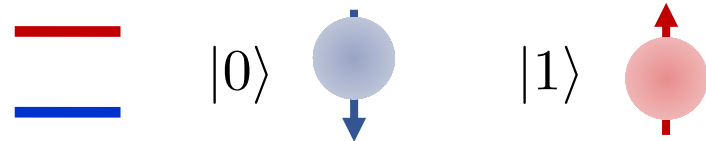
Richard Feynman

"Creating machines based on the laws of quantum mechanics instead of the laws of classical physics." (1982)

[+ Benioff, Manin]

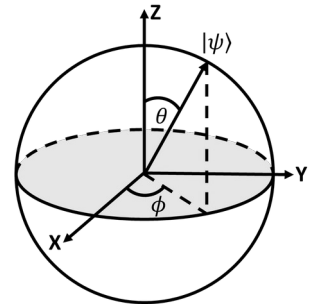
qubit = quantum bit

data units:



valid states:

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle \oplus \sin \frac{\theta}{2} e^{i\phi} |1\rangle$$



operations:

unitary

1-qubit

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$$

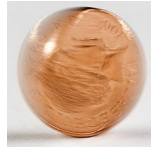
$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

2-qubits

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ What does that mean? **Quantum superposition**

Spinning coin analogy



Measurement



Probability \propto

$$|\alpha|^2$$



$$|\beta|^2$$

Schrodinger's cat

$$\frac{1}{\sqrt{2}}|\text{cat}\rangle + \frac{1}{\sqrt{2}}|\text{no cat}\rangle$$

$$P_{\text{dead}} = 1/2$$

$$P_{\text{alive}} = 1/2$$

How about **entanglement**?

Two coins



Possible outcomes

Entangled coins/states:

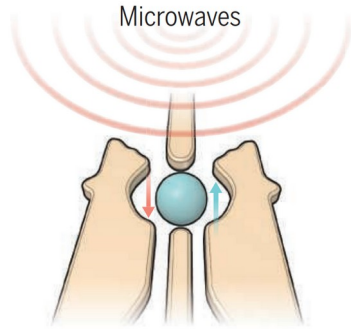
- Obtaining H/T for the first \rightarrow defines the outcome of the second

Ex.: $|\phi^+\rangle = \frac{1}{\sqrt{2}} (|\text{heads heads}\rangle + |\text{tails tails}\rangle)$

- Coins can no longer be thought of being independent, they are *entangled*
- Curiosity:** 300 coins $\rightarrow 2^{300} \approx 10^{90}$ states $>$ # atoms in the universe $\approx 10^{80}$

Existing qubit platforms

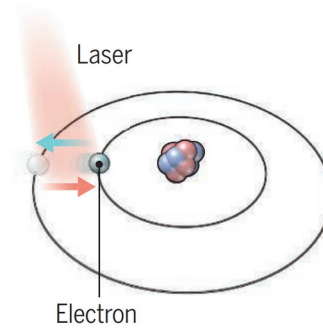
Silicon quantum dots



- “Artificial atoms” made by adding an electron to a small piece of pure silicon.
- Microwaves control the electron’s quantum state.

Intel, HRL, QuTech
UNSW, Delft, RIKEN, ...

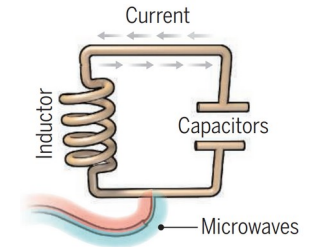
Trapped ions



- Ions, have quantum energies that depend on the location of electrons.
- Tuned lasers cool and trap the ions, and put them in superposition states.

IonQ, Honeywell
Maryland, ...

Superconducting loops

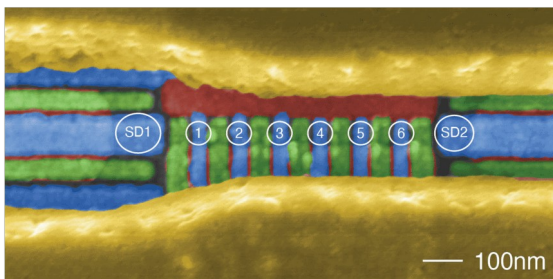


- Resistance-free current oscillates back and forth around a circuit loop
- Injected microwave signal excites the current into superposition states
- Emulates a quantum anharmonic oscillator

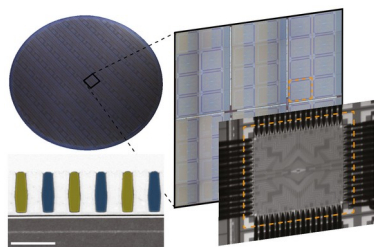
Google, IBM, ...
ZJU, UESTC, ...

Building many of them – Noisy intermediate quantum devices

Silicon quantum dots

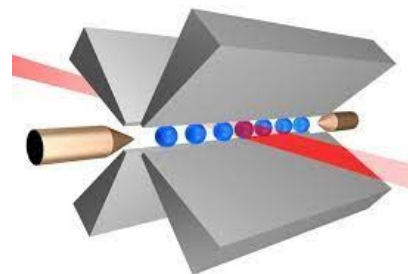
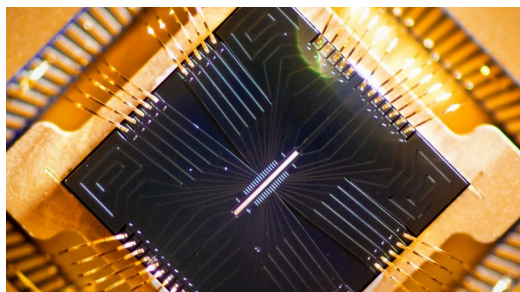


[Qutech 2022]



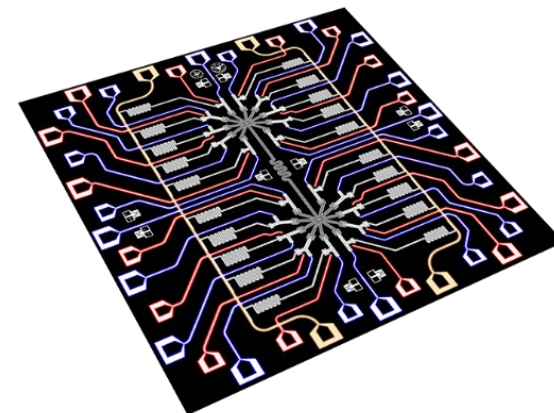
[Intel 2024]

Trapped ions

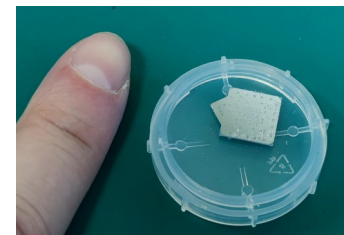


[Maryland, IonQ]

Superconducting quantum circuits

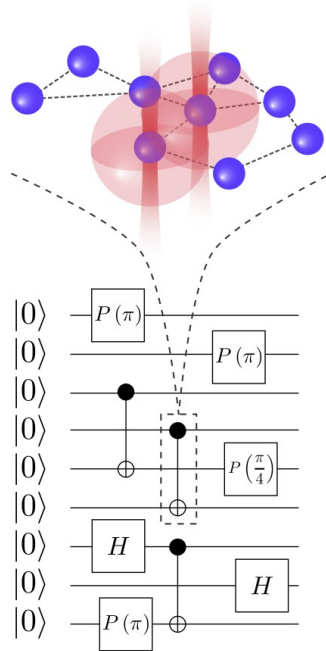


[IOP, ZJU]



How it works?

Digital

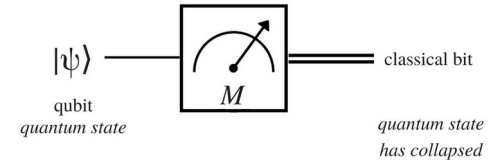


[QuEra Computing Inc.]

- Platform agnostic
- Possibility of error detection/correction

Qubits are “measured”

Measurements ‘destroys’ the quantum state.



bitstring

0
1
0
1
1
0
0
0

Composing many shots



probability of each string

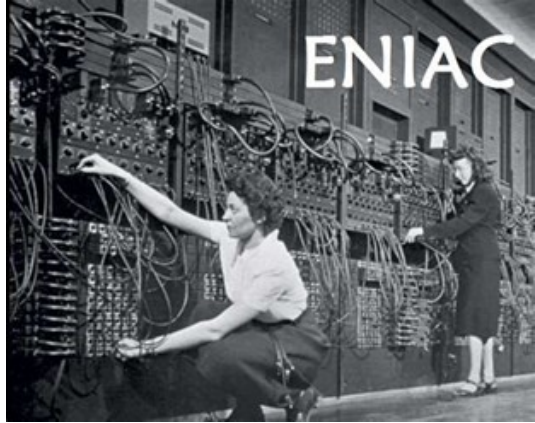


reconstruct the final state

Large number of states → small output

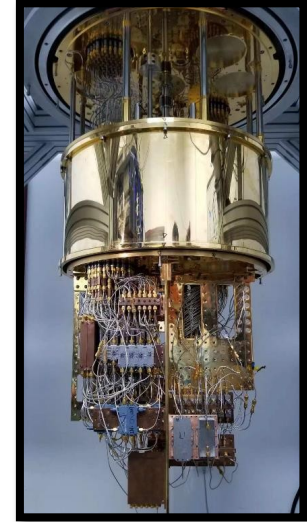
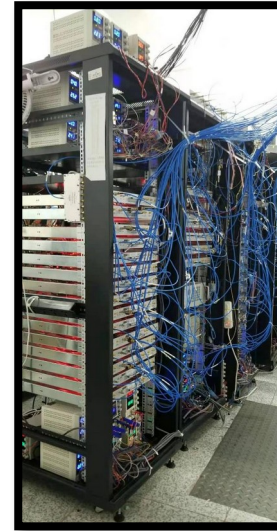
The more things change, the more they stay the same...

First general-purpose digital computer

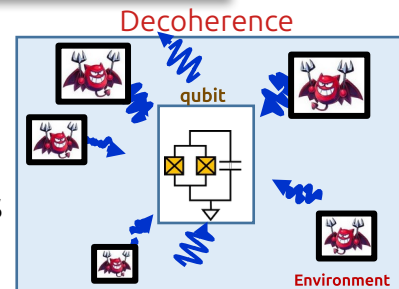


- 30 tons
- 18,000 vacuum tubes
- 1,500 relays
- +100,000 of resistors, capacitors and inductors, = add or subtract 5,000 times per second!

SC quantum circuit



- 36-qubits (121 available)
- Fully programmable
- Emulates dynamics of \hat{H} with $\dim = 9B$ states
- Operates at 20mK...

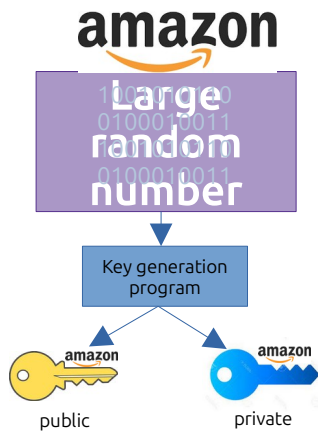


Quantum Computers: What Are They Good For?

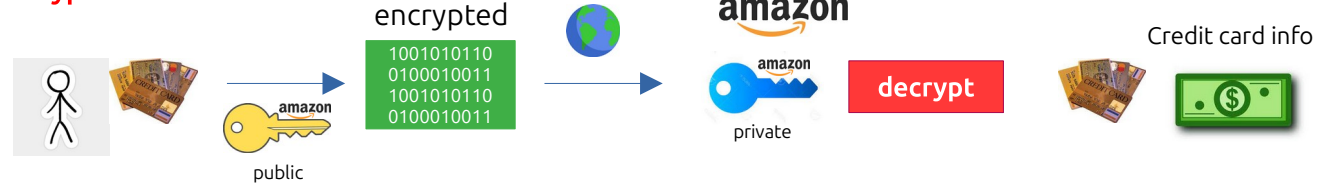
- ✓ Quantum processing
- ✓ Quantum communication
- ✓ Quantum memory

Code cracking – factoring large prime numbers

1) Key generation



2) encrypted transmission



Based on: $(m^e)^d \equiv m \pmod{n}$ where

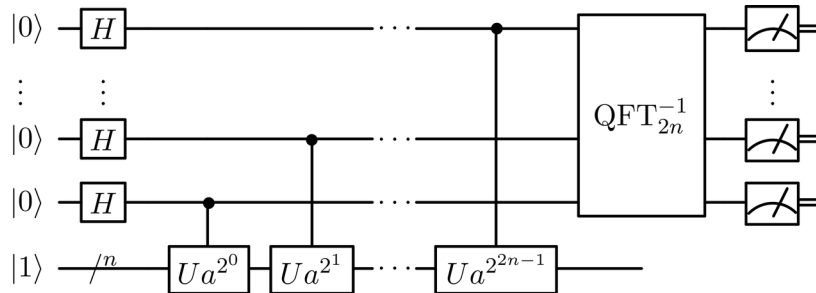
Prime numbers
 $n = pq$



→ (n, e) Scrambles the data

→ To unscramble, one needs one of the primes

- **Shor algorithm** – quantum circuit to find prime factors of an integer +classical routines



In practice: n = 15 or 21 have been demonstrated so far

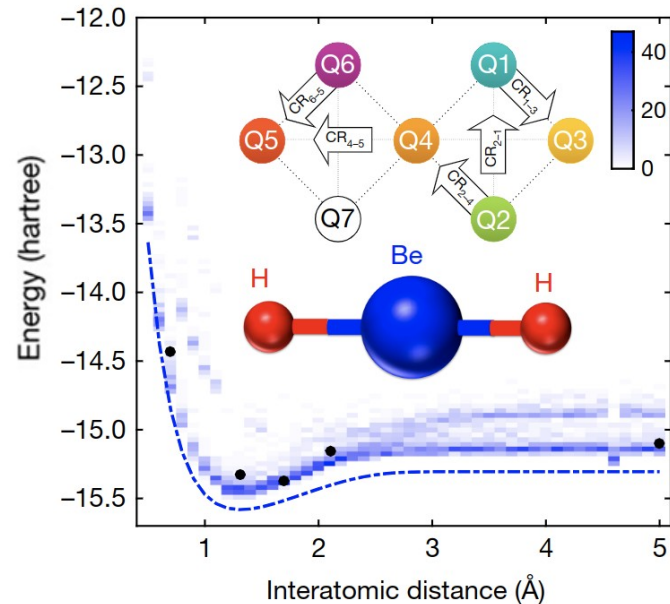
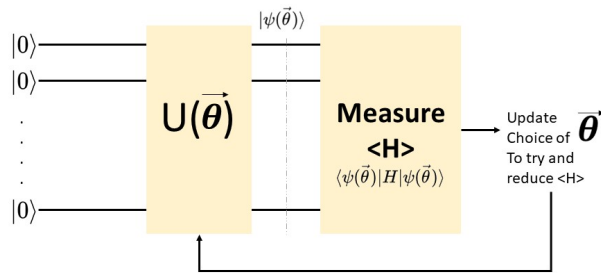
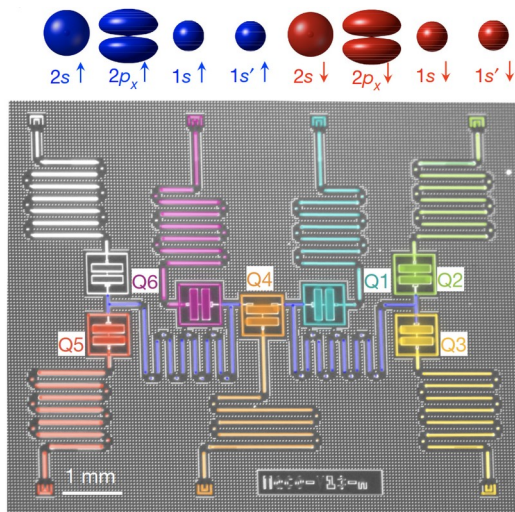
[Nature 414, 883 (2001)]
 [Nature Photonics 6, 773 (2012)]

Quantum Computational Chemistry

→ Finding the **lowest energy states of molecules** – dictates the structure of the molecule and how it will interact with other molecules.

→ critical for chemists to **design new molecules**, **reactions**, and chemical **processes** for industrial applications.

Iterative (hybrid) algorithm: Variational Quantum Eigensolver

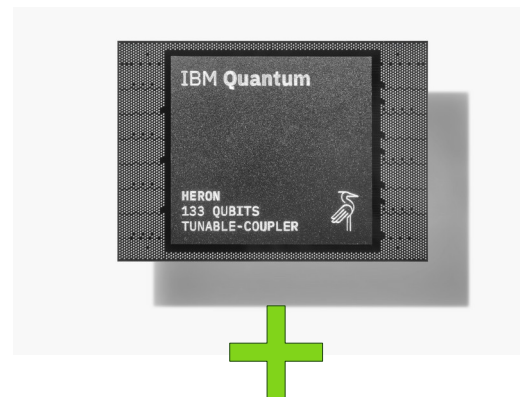
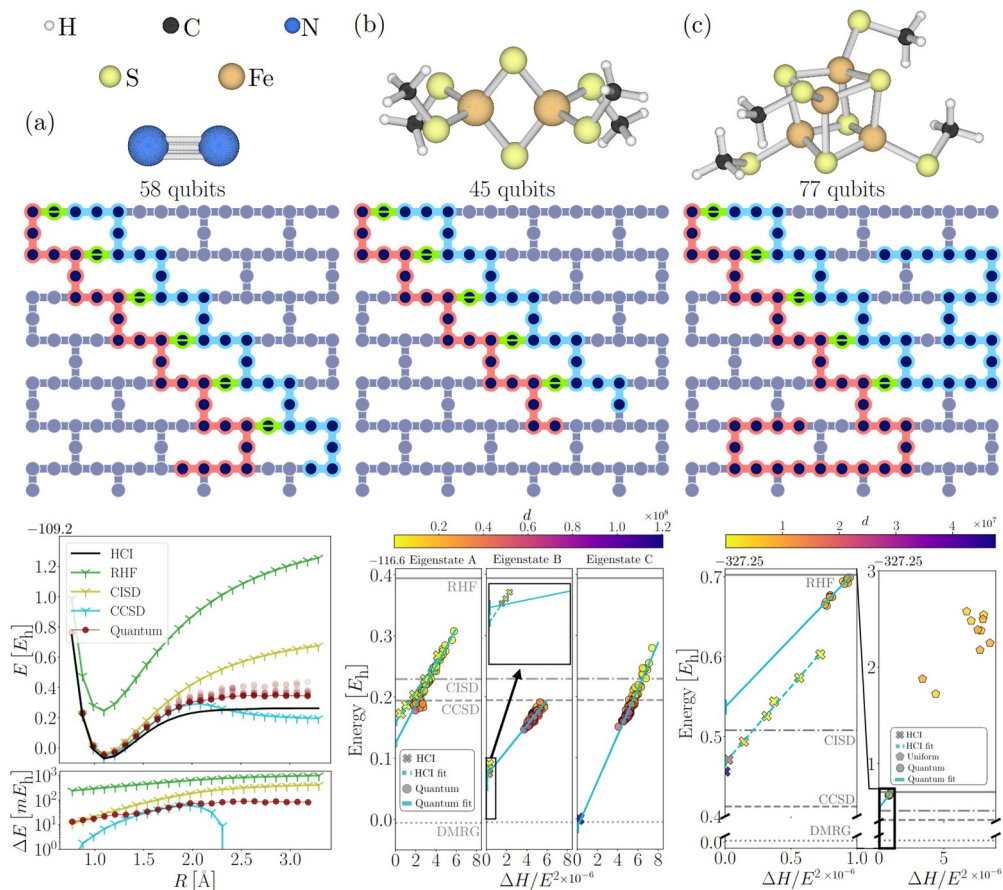


[Kandala et al. Nature 549, 242 (2017)]

[See also Science 369, 1084 (2020) Google's in H₁₂ chains]

Quantum Computational Chemistry – last month's (preprint)

Robledo-Moreno et al. "Chemistry Beyond Exact Solutions on a Quantum-Centric Supercomputer"
arXiv:2405.05068



Quantum Finance?



nature reviews physics

Explore content ▾ About the journal ▾ Publish with us ▾ Subscribe

nature > nature reviews physics > review articles > article

Review Article | Published: 11 July 2023

Quantum computing for finance

Dylan Herman , Cody Googin, Xiaoyuan Liu, Yue Sun, Alexey Galda, Ilya Safro, Marco Pistoia & Yuri Alexeev

Nature Reviews Physics 5, 450–465 (2023) | [Cite this article](#)

npj | Quantum Information



ARTICLE OPEN

Quantum risk analysis

Stefan Woerner ¹ and Daniel J. Egger¹

→ Applications for finance problems, such as portfolio optimization, risk estimation ...

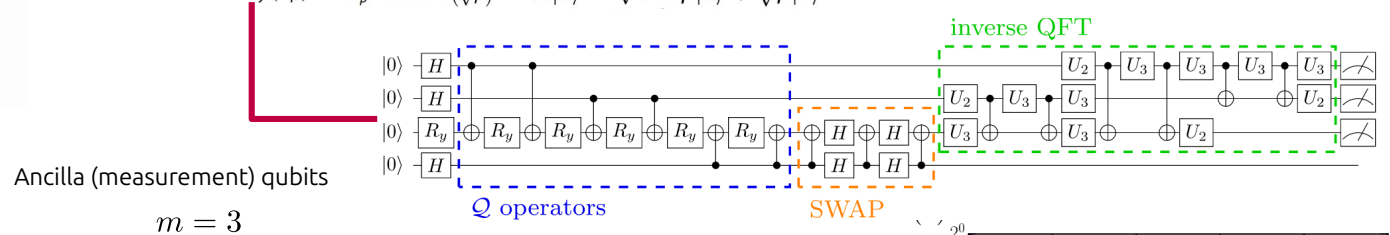
Quantum Amplitude Estimation → used to estimate risk measures with a quadratic speed-up over classical Monte Carlo simulation.

Example:

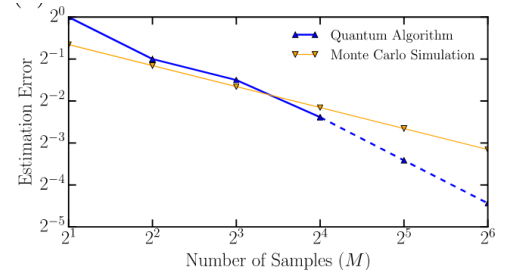
Mean value of a bond with a given probability of rate change $r \rightarrow \delta r$

$$V = \frac{(1-p)V_F}{1+r+\delta r} + \frac{pV_F}{1+r} = (1-p)V_{\text{low}} + pV_{\text{high}}$$

$$\mathcal{A} = R_y(\theta_p) \quad \theta_p = 2 \sin^{-1}(\sqrt{p}) \quad \mathcal{A}|0\rangle = \sqrt{1-p}|0\rangle + \sqrt{p}|1\rangle$$



M samples	Error
Quantum Algorithm	$\mathcal{O}(M^{-1})$
Monte Carlo	$\mathcal{O}(M^{-1/2})$



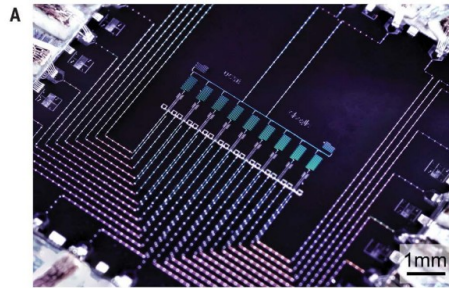
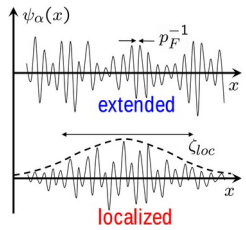
[Woerner, Egger npj Quantum Information (2019)5:15]

Solving (or giving hints) on some very hard Physics problems

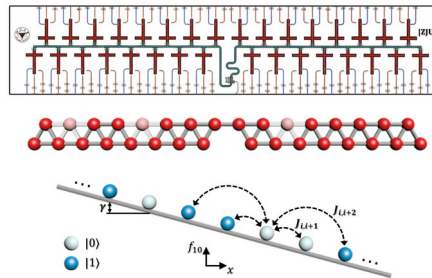


→ Localization of quantum particles in the presence of interactions (many-body localization)

Localization under disorder + interactions

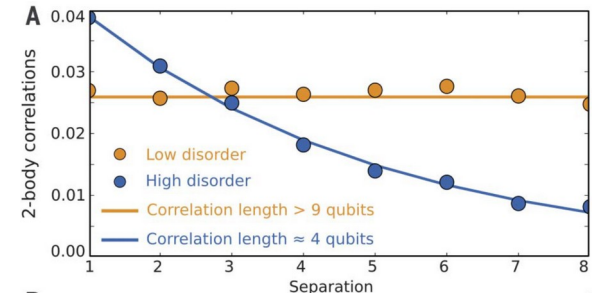
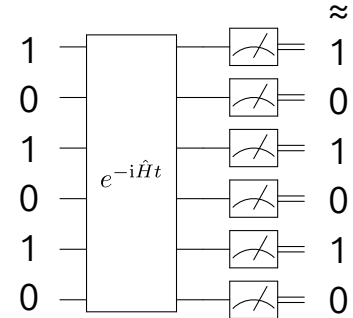


[Roushan *et al.*, *Science* **358**, 1175 (2017)]



[Guo, ..., *RM** *Phys. Rev. Lett.* **127**, 240502 (2021)]

Loosely speaking



[Neil *et al.* *Science* **360** (6385), 195 (2018)]



Nobel Prize 1977



PW Anderson

Local quantum memory? Maybe we don't need a quantum computer for that...

[see also Guo, *RM**, *Nature Physics* **17**, 234 (2021)]

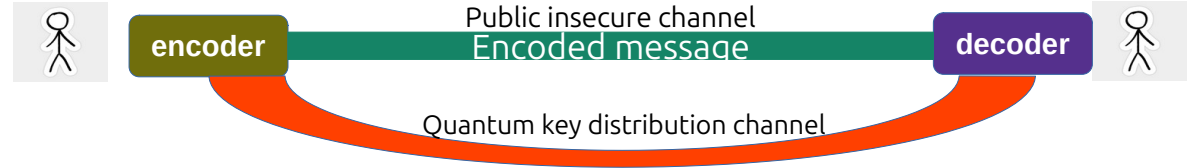
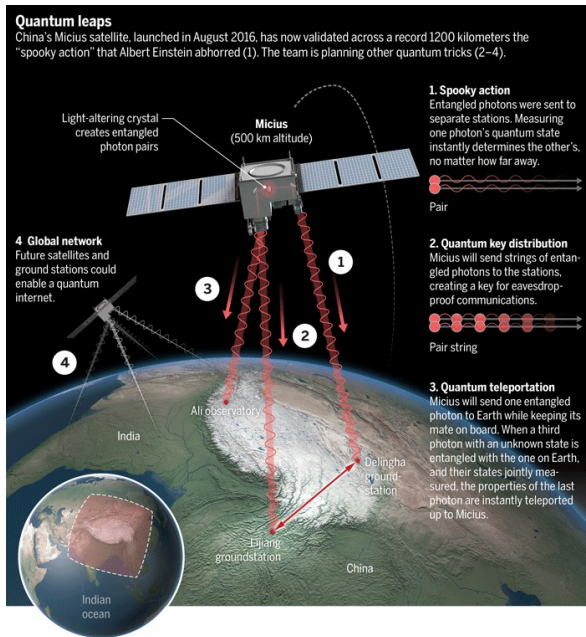
Quantum Communication

- Probing entanglement at large distances



Pair of entangled photons sent to receivers 1200km (~745 miles) apart
→ one photon's quantum state instantly determines the other's

- Quantum key distribution

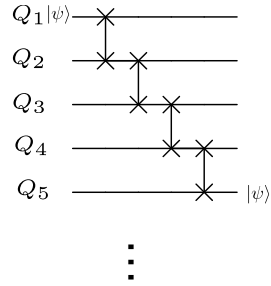


act of **measurement** of an eavesdropper destroys the key!

Can we investigate the "channel" as a "quantum wire"?
Quantum state transfer!

Quantum Communication - quantum state transfer in a quantum computer

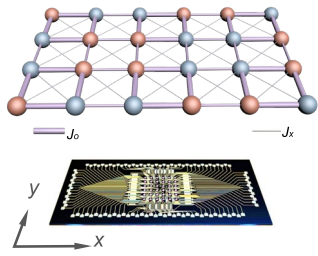
“SWAP train”



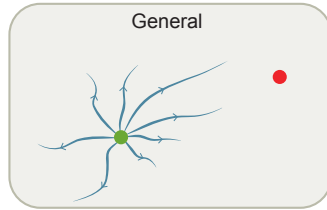
$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

: Swaps the state of two qubits

- Or: Multigate Hamiltonian evolution – “analog” mode – hybrid computation



Fock space

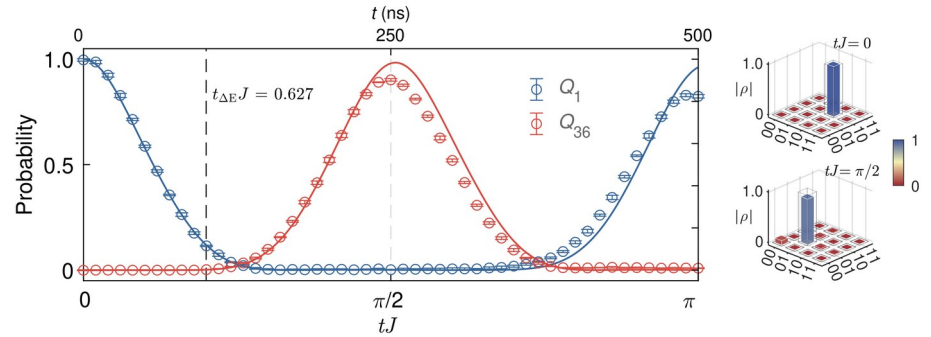
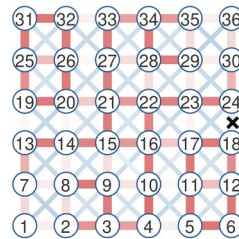


General

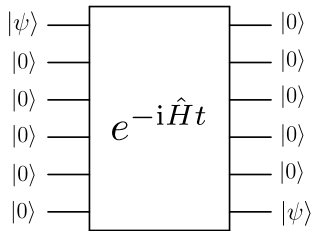
- Transfer of two-qubits maximally entangled states

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

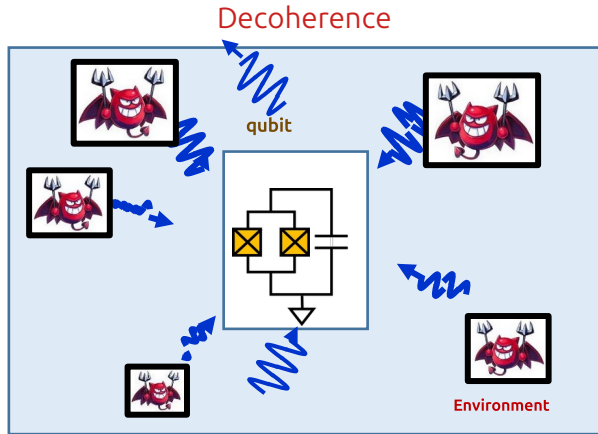
6x6:



[L. Xiang, ..., **RM***, Scalettar, Nat. Comm. 15 4918 (2024)]



What is the bottleneck? Quantumness of Qubits don't last long and gates are not perfect...

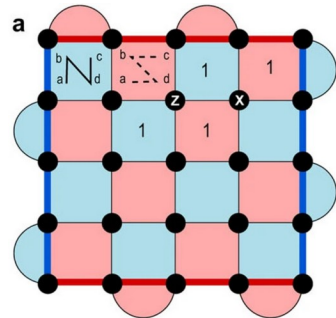


→ Solution:

- Quantum error correction
- Physical vs. **Logical qubits**

+noise

Several qubits working together as one to represent one qubit of information



- Data qubit
- Z-parity check
- X-parity check
- Logical Z boundary
- Logical X boundary

→ **The goal:** even if one physical qubit “fails”, the remainder in the logical set recovers the information

- Set of **data encoding** + **low-depth checks** to ensure the information is preserved
- Active area of research and demonstration!

→ eg: “*Suppressing quantum errors by scaling a surface code logical qubit*” Google Quantum AI*, Nature **614**, 676 (2023)

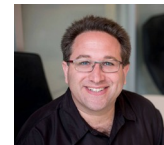
[Gambetta, Chow, Steffen npj Quantum Information 3, 2 (2017)]

Take away message

Thank you!

- Quantum computers algorithmically apply the standard laws of quantum mechanics
- Search of new problems **and** corresponding algorithms that can be implemented in QC's is a field of intense research
- **Avoid the hype:** Quantum computers will likely not replace our classical computers any time soon. They are often designed for very specific tasks, and are doing so (currently) sub-optimally
- **But there are many fun things that they can accomplish!**

"If you don't talk to your kids about quantum computing... someone else will."



Scott Aaronson (UT Austin)

Extra slides

Monte Carlo comes to the rescue!

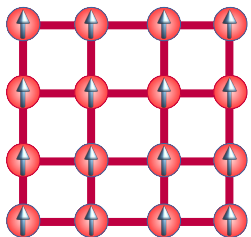
Ising model

$$E_{\{S\}} = -J \sum_{\langle i,j \rangle} S_i S_j, \quad S_i = \pm 1$$

$$p_{\{S\}}(T) \propto e^{-E_{\{S\}}/T}$$

Annealing: $T_{\text{high}} \rightarrow T_{\text{low}}$ proposing spin flips

Provides search to a low-energy configuration



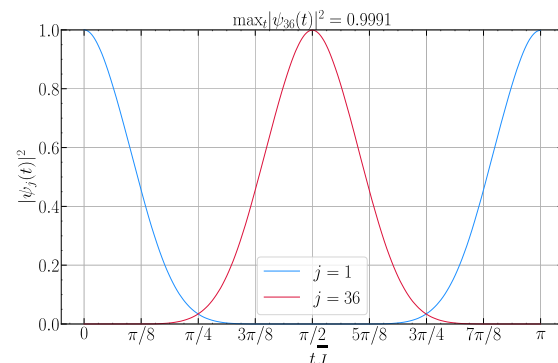
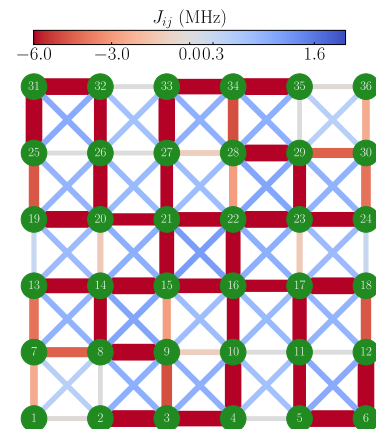
Quantum state transfer

$$\tilde{F}(t^*) = 1 - |\langle \psi(t^*) | \psi_{\text{target}} \rangle|^2 \quad \text{with} \quad |\psi(t^*)\rangle = e^{-i\hat{H}t^*} |\psi(0)\rangle$$

$$p_{\{J_{ix}, J_{iy}, J_x\}} \propto e^{-\tilde{F}/T}$$

Annealing: $T_{\text{high}} \rightarrow T_{\text{low}}$ proposing $\{J_{ix}, J_{iy}\}$ changes

Provides search to configuration that maximizes QST



Transmon qubit:

LC oscillator

Classically

$$H = \frac{1}{2}CV^2 + \frac{1}{2}LI^2$$

$$(m = C \quad \omega = 1/\sqrt{LC} \rightarrow H = p^2/2m + m\omega^2x^2/2)$$

Quantum

$$\hat{H} = 4E_C\hat{n}^2 + \frac{1}{2}E_L\phi^2$$

$$E_C = e^2/(2C)$$

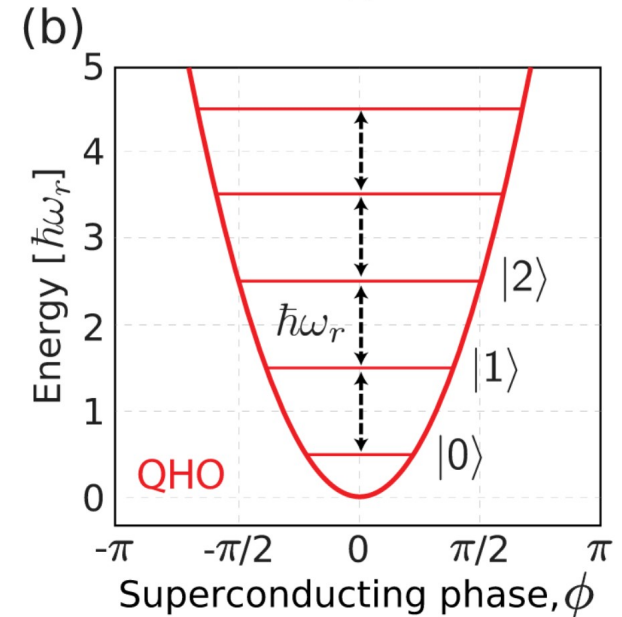
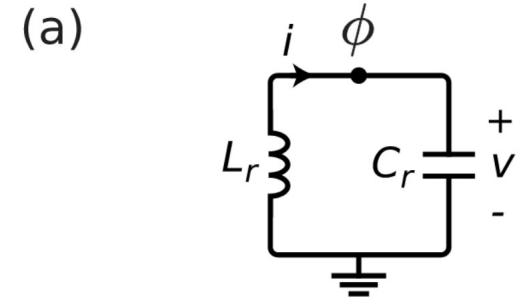
$$n = n_{zpf} \times i(a - a^\dagger)$$

$$\hat{E}_L = (\Phi_0/2\pi)^2/L$$

$$\phi = \phi_{zpf} \times (a + a^\dagger)$$

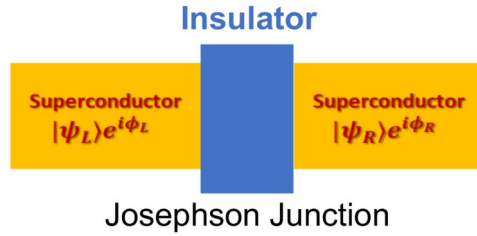
- equally spaced energy levels
- no selectivity

Second quantization: $H = \hbar\omega_r \left(a^\dagger a + \frac{1}{2} \right) \quad \omega_r = \sqrt{8E_L E_C}/\hbar = 1/\sqrt{LC}$



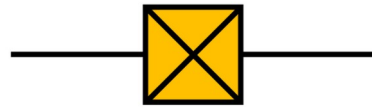
Transmon qubit:

Anharmonic LC oscillator



$$I = I_c \sin(\phi), \quad V = \frac{\hbar}{2e} \frac{d\phi}{dt}$$

nonlinear inductance

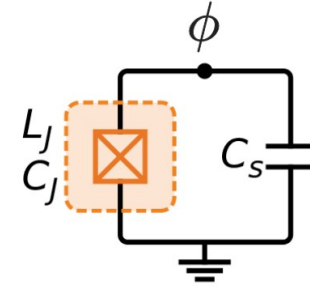


$$L_J = \frac{\Phi_0}{2\pi\sqrt{I_c^2 - I^2}}$$

$$H = 4E_C n^2 - E_J \cos(\phi)$$

$$\frac{H}{\hbar} = \omega_{10}|1\rangle\langle 1| + (2\omega_{10} + \eta)|2\rangle\langle 2|$$

(c)



(d)

