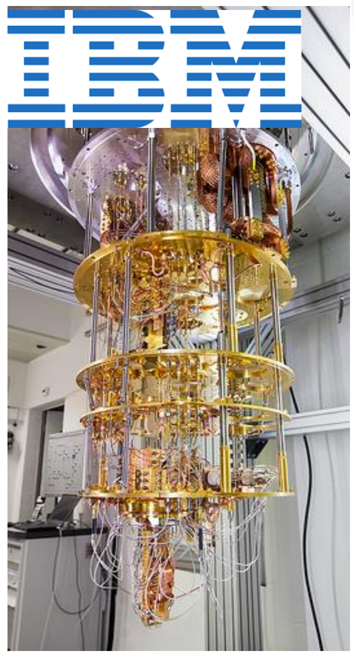
Quantum Computers: What, Why, and When?

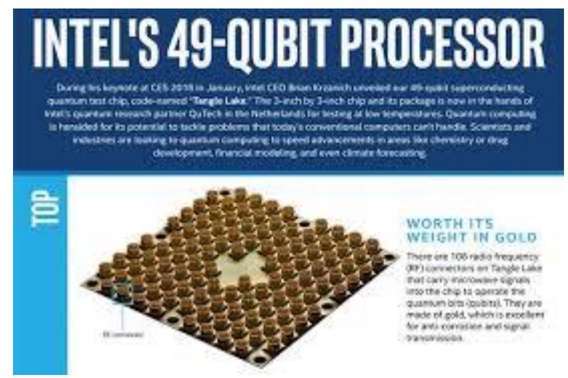
Moshe Goldstein

אוניברסיטת תל-אביב
TEL AVIV UNIVERSITY

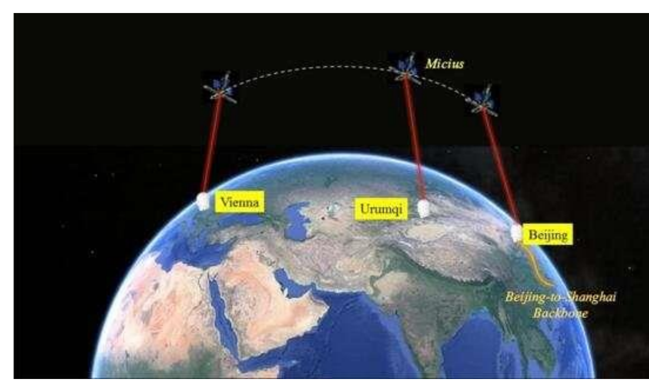
Some recent news

- Big companies





- And governments



Outline

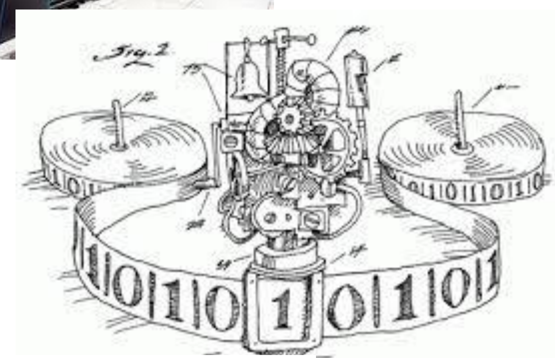
- Classical computation
- Quantum computation
  - The idea
  - Power & limitations
  - Architectures

Classical Computers

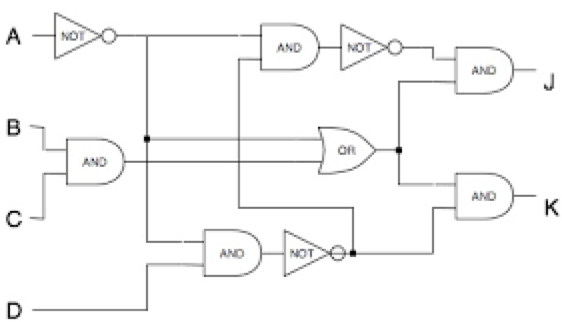
- As we know them

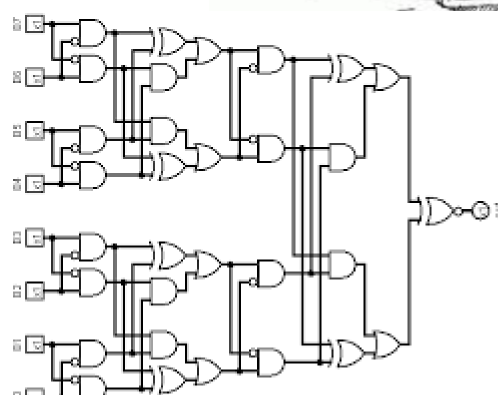


- In computer science
  - **Turing machine**
  - **boolean circuit**
  - and others **…**



0/1
0/1
0/1
0/1

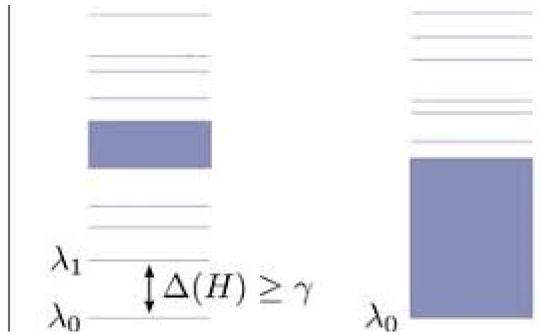


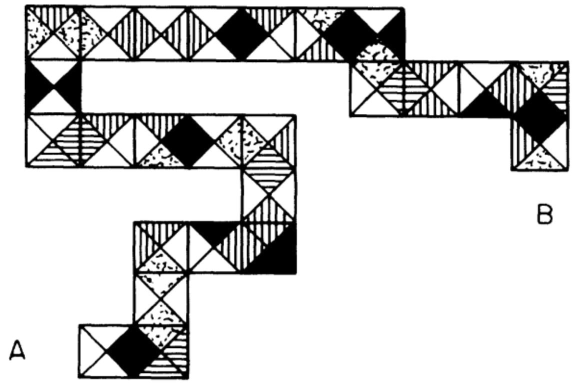


- **Church-Turing**: all **equivalent** (and as **efficient**)

Computational Problems

- Uncomputable:
  - **halting problem**
  - some **domino snakes**
  - **spectral gap** ...



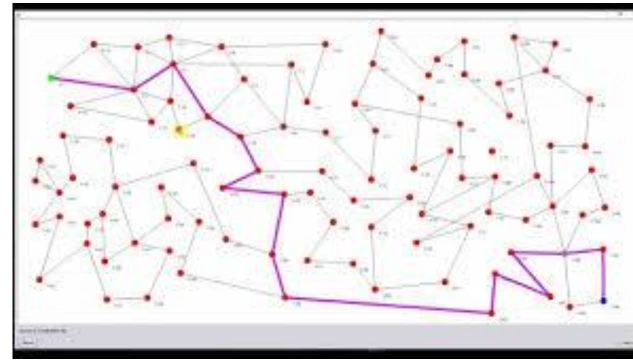


- Computable:

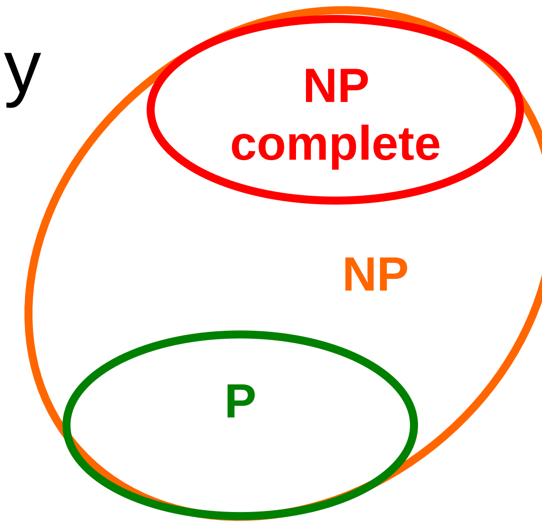
		$N = 10$	$N = 20$	$N = 100$	$N = 101$
Polynomial (P)	N	10	20	100	101
	N^2	100	400	10000	10201
Exponential (EXP)	2^N	1024	$\approx 10^6$	$\approx 10^{30}$	$\approx 2 \cdot 10^{30}$

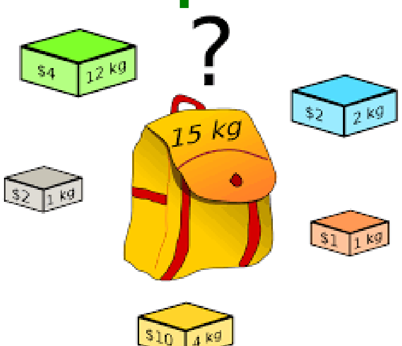
P vs NP

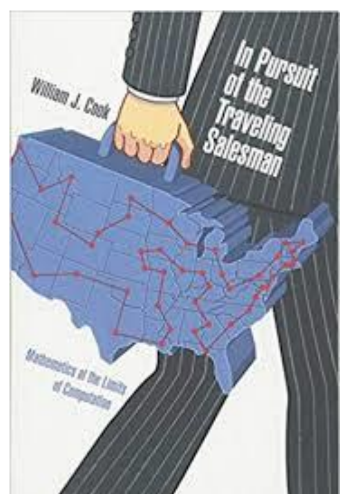
- Polynomial problems (**P**):
  - **searching** in a list
  - **sorting**
  - **shortest path …**



- **NP**: solutions can be **checked** easily
  - **P vs. NP** ($1,000,000 question!)
- **NP complete**
  - **Traveling salesman**
  - **Knapsack**



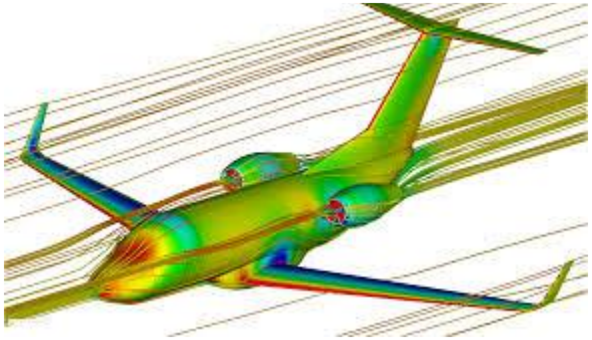




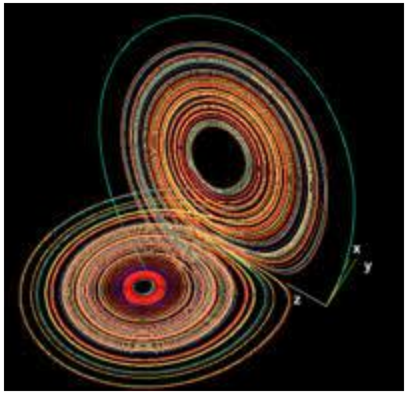
See also:
Douglas Hofstadter, *Gödel, Escher, Bach: an Eternal Golden Braid*
דוד הראל, המחשב אינו כל יכול

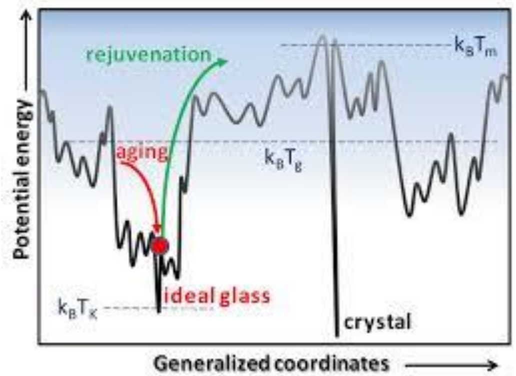
Computational Physics?

- **Classical**: typically polynomial (**P**)
  - **mechanics**
  - **fluid dynamics**
  - **electromagnetism**
  - **general relativity**



- **Caveats**:
  - **chaos** (**weather** …)
  - **glasses** (**NP**)



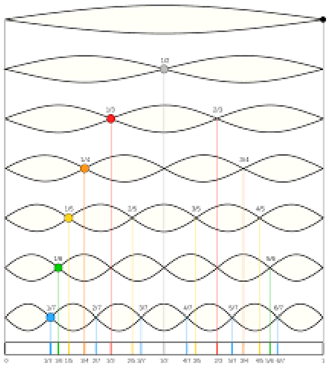


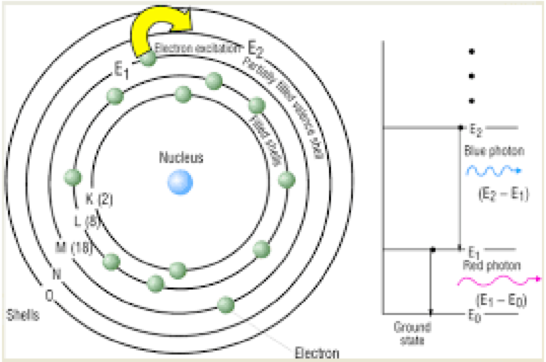
Outline

- Classical computation
- Quantum computation
  - The idea
  - Power & limitations
  - Architectures

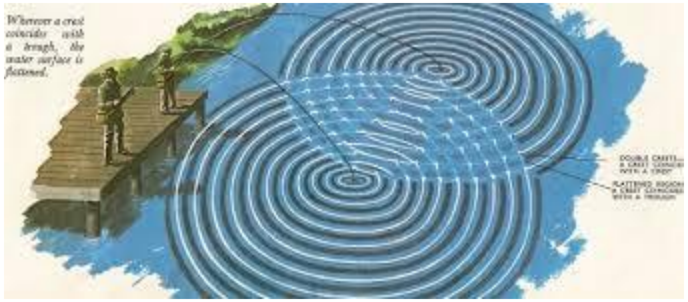
The Quantum World (I)

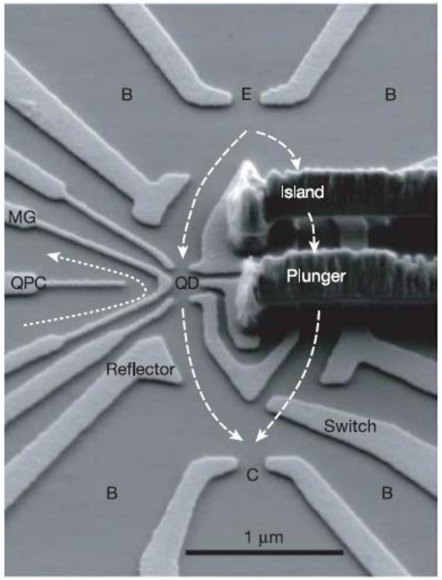
- **Everything** is **both particle** and **wave**
  - **discrete energy levels**

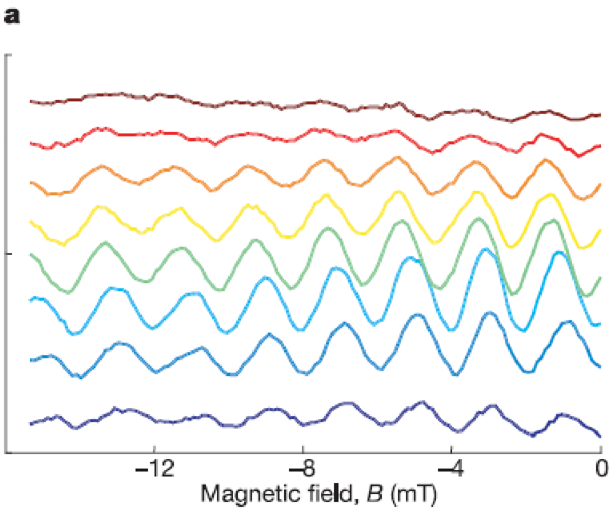




  - **interference**



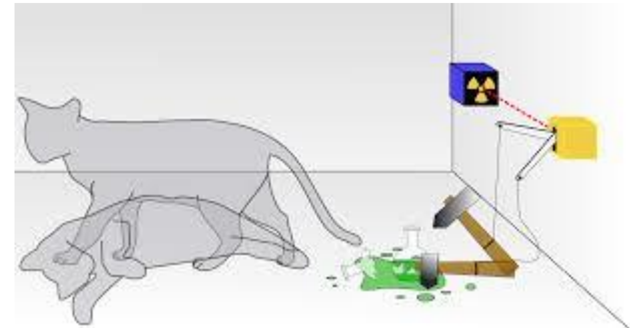




[Heiblum]

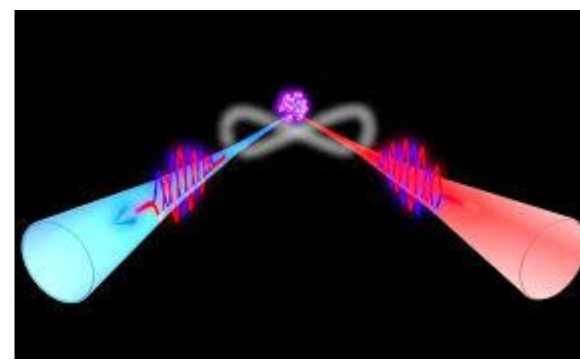
The Quantum World (II)

- **Waves** of **probability !**
  - **measurement defines** the quantity
  - **observation affects** the system
  - **decoherence**



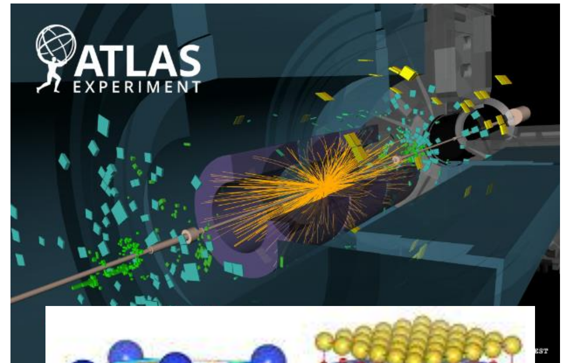
- **Many** particles: **entanglement**
  - "**spooky action at a distance**"

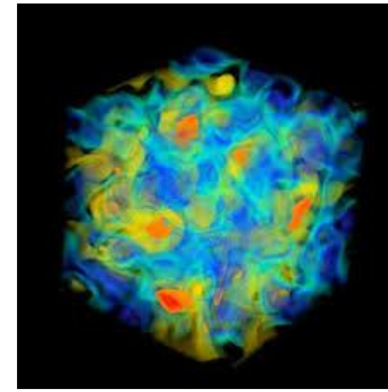
$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$



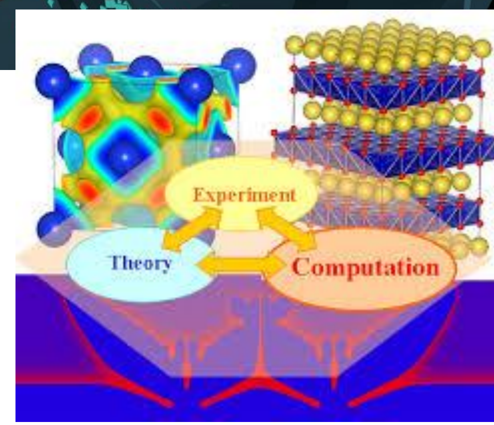
Computational Quantum Physics

- **Many** particle systems
  - **particle physics**

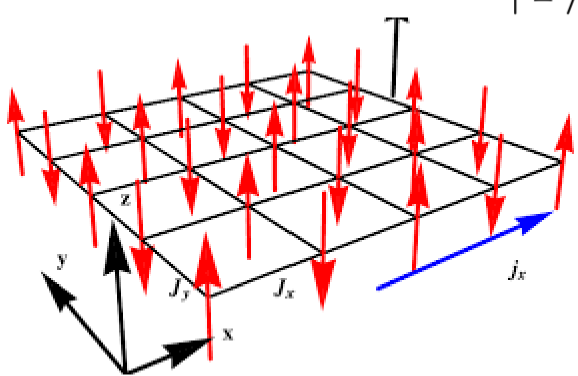




  - **materials science**



- **Exponential state space !**



$$\left.\begin{aligned} |\Psi\rangle = & c_{00\cdots000}|00\cdots000\rangle + \\ & c_{00\cdots001}|00\cdots001\rangle + \\ & c_{00\cdots010}|00\cdots010\rangle + \\ & \vdots \\ & c_{11\cdots111}|11\cdots111\rangle \end{aligned}\right\} \textbf{2^N terms!}$$

Quantum Computing?

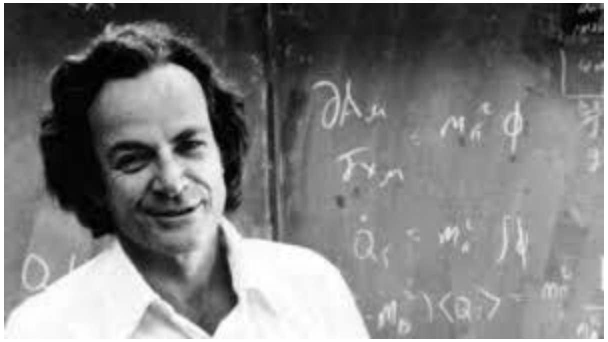
- **Feynman** (**1981**; see also **1959**):

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981



4. QUANTUM COMPUTERS—UNIVERSAL QUANTUM SIMULATORS

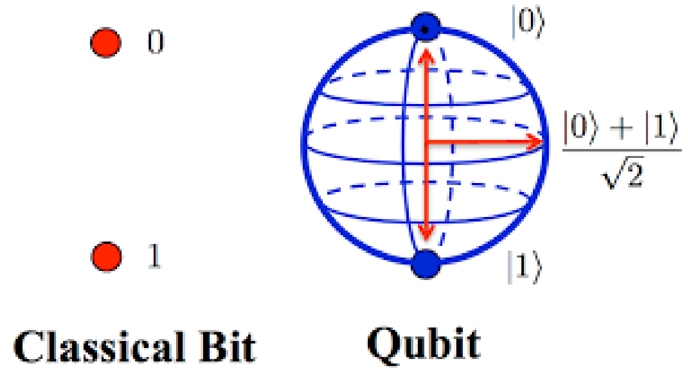
  - **quantum systems find their states**
  - **use quantum system** for **computation !**

$$\left.\begin{aligned}|\Psi\rangle = & \, c_{00\cdots000}|00\cdots000\rangle + \\ & \, c_{00\cdots001}|00\cdots001\rangle + \\ & \, c_{00\cdots010}|00\cdots010\rangle + \\ & \qquad\vdots \\ & \, c_{11\cdots111}|11\cdots111\rangle\end{aligned}\right\} 2^N \text{ terms!}$$

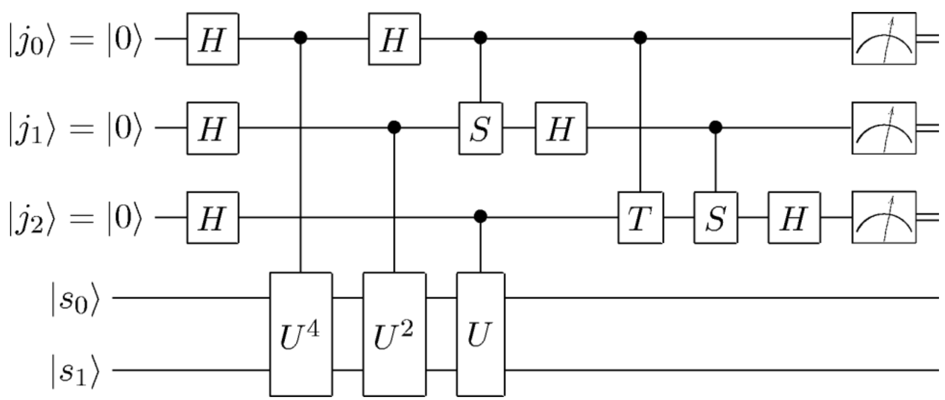
See also:
Benioff (1980); Manin (1980)

Quantum Computer

- **Quantum circuit**:
  - **qubits**



  - **quantum gates**



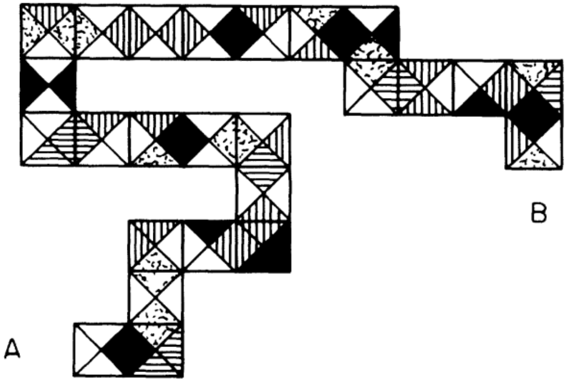
  - **measurement** (probabilistic, bounded error: BPP vs. BQP)

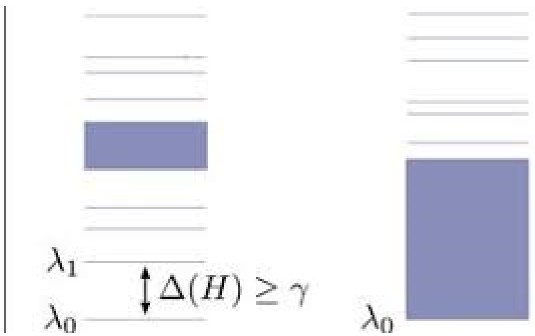
Outline

- Classical computation
- Quantum computation
  - The idea
  - Power & limitations
  - Architectures

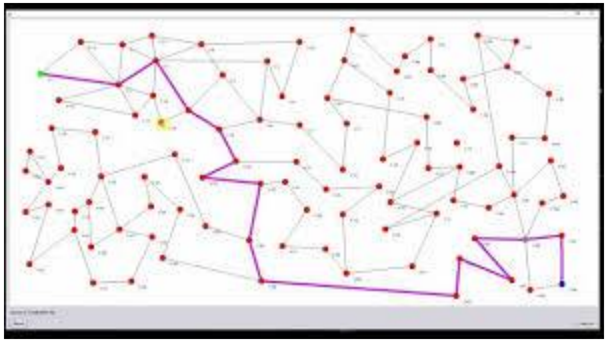
What Can It Do?

- **Uncomputable** problems? **No!**

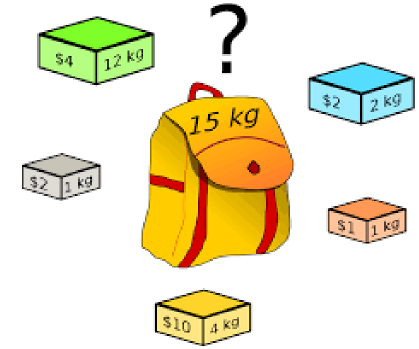




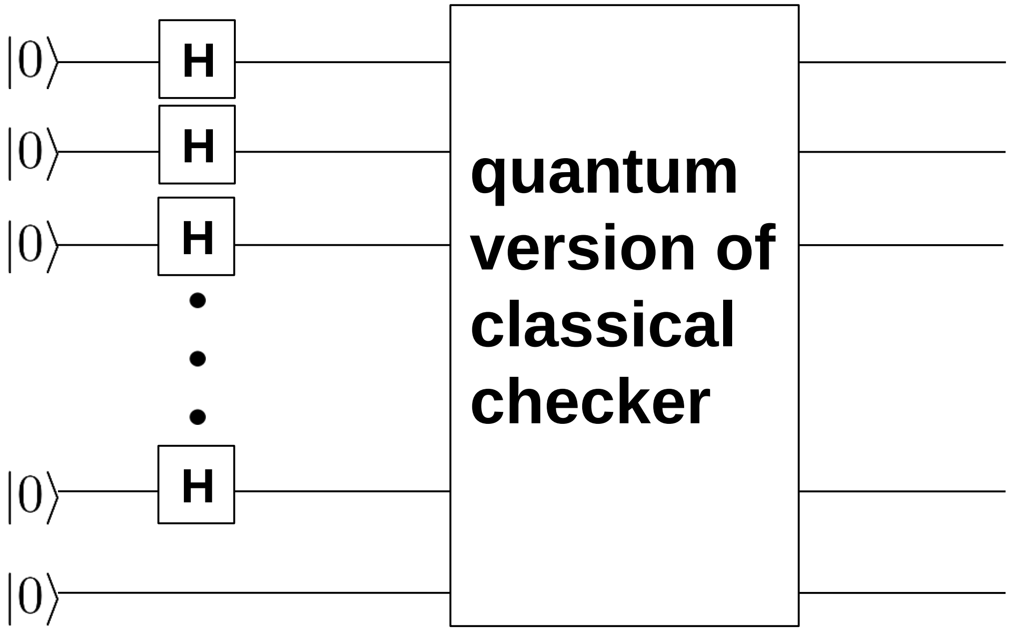
- **Classically computable** problems? **Yes!**
  - **Nontrivial**: **QC** is **reversible**
  - **Nontrivial**: **superposition!**



Solve NP?



- Can check **all solutions at once**!



$$
\begin{aligned}
|\Psi\rangle = & 2^{-N/2}|00\cdots000;0\rangle + \\
& 2^{-N/2}|00\cdots001;0\rangle + \\
& 2^{-N/2}|00\cdots010;1\rangle + \\
& 2^{-N/2}|00\cdots011;0\rangle + \\
& \vdots \\
& 2^{-N/2}|11\cdots111;0\rangle
\end{aligned}
$$

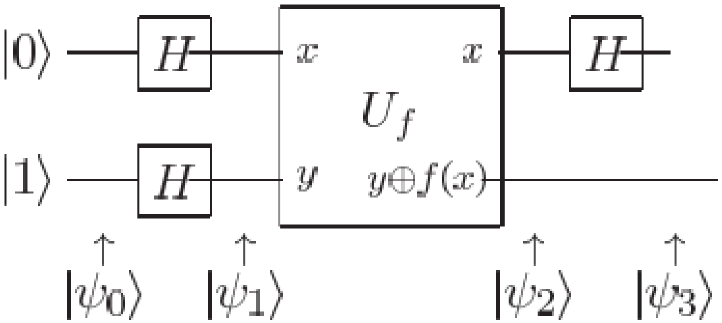
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- **But**: **measurement** success probability is $1/2^N$
  - **no improvement!**
  - related: **Holevo bound**

Toy Example: Deutsch

- **Problem**:
  - Input: 1-bit function $f : \{0,1\} \rightarrow \{0,1\}$
  - Output: $f(0) \oplus f(1)$ (equal or different)

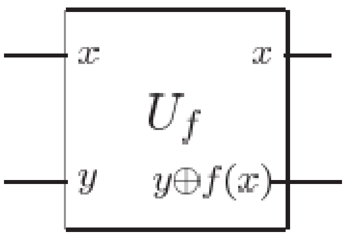
- **Solution**:
  - Classical: 2 calls
  - Quantum: 1 call!

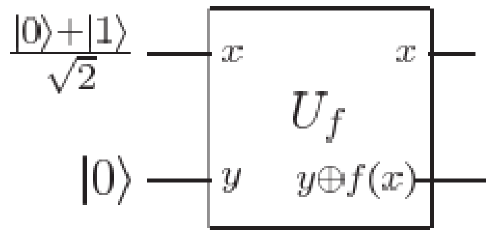


Toy Example: Details

- **Unitary** implementation of f:

$$|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$$

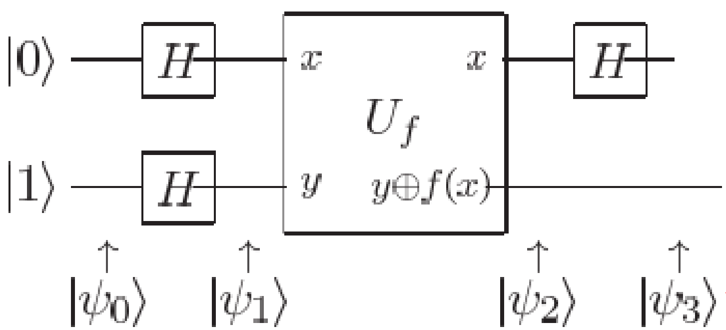




$$|\psi\rangle = \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$$

- **Deutsch's algorithm**:

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



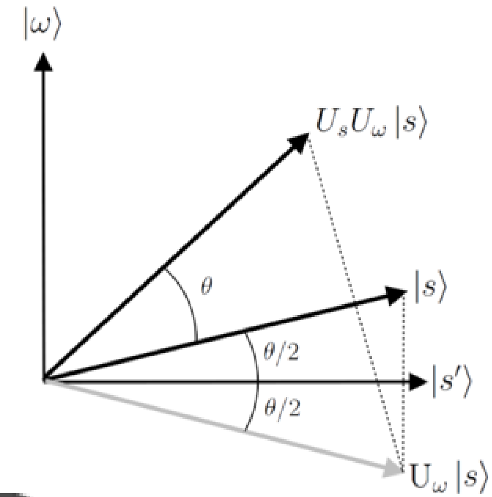
$$|\psi_3\rangle = \begin{cases} \pm|0\rangle \dfrac{|0\rangle - |1\rangle}{\sqrt{2}} & f(0) = f(1) \\ \pm|1\rangle \dfrac{|0\rangle - |1\rangle}{\sqrt{2}} & f(0) \neq f(1) \end{cases}$$

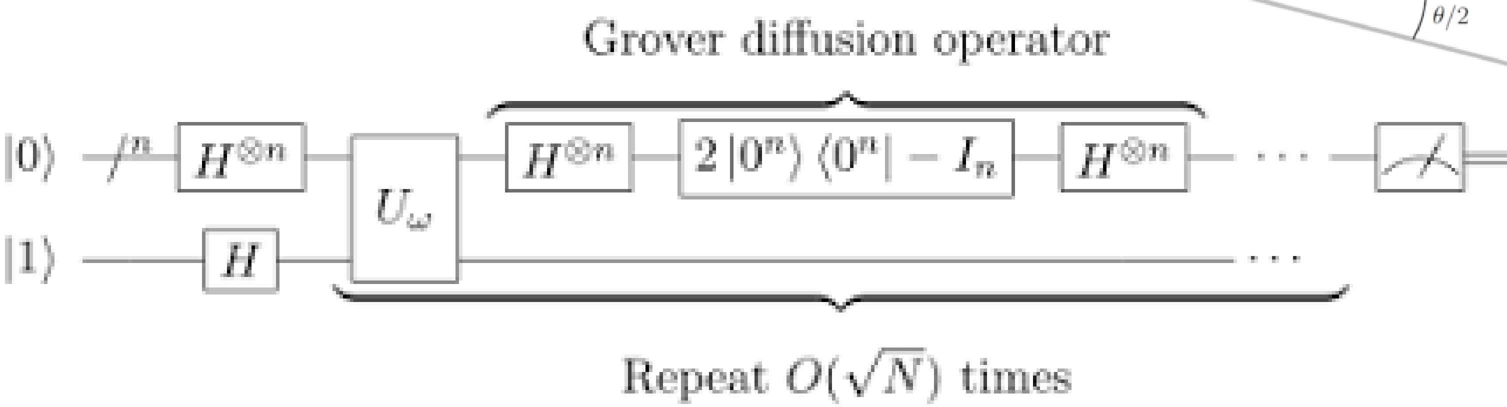
$$|\psi_2\rangle = \begin{cases} \pm\dfrac{|0\rangle + |1\rangle}{\sqrt{2}} \dfrac{|0\rangle - |1\rangle}{\sqrt{2}} & f(0) = f(1) \\ \pm\dfrac{|0\rangle - |1\rangle}{\sqrt{2}} \dfrac{|0\rangle - |1\rangle}{\sqrt{2}} & f(0) \neq f(1) \end{cases}$$

$$|\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

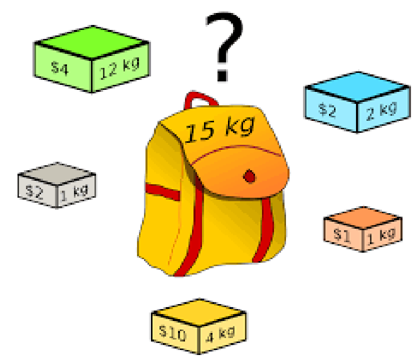
Quantum Search

- **Grover**'s algorithm (**1996**)
  - search length N list in $\sqrt{N}$ time **!**





- Solve **NP** in time $2^{N/2}$
  - Probably maximal improvement

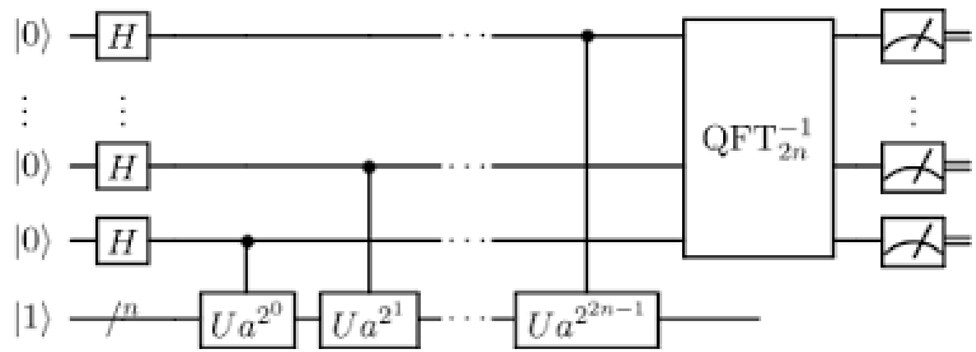


Shor's Algorithm (1994)

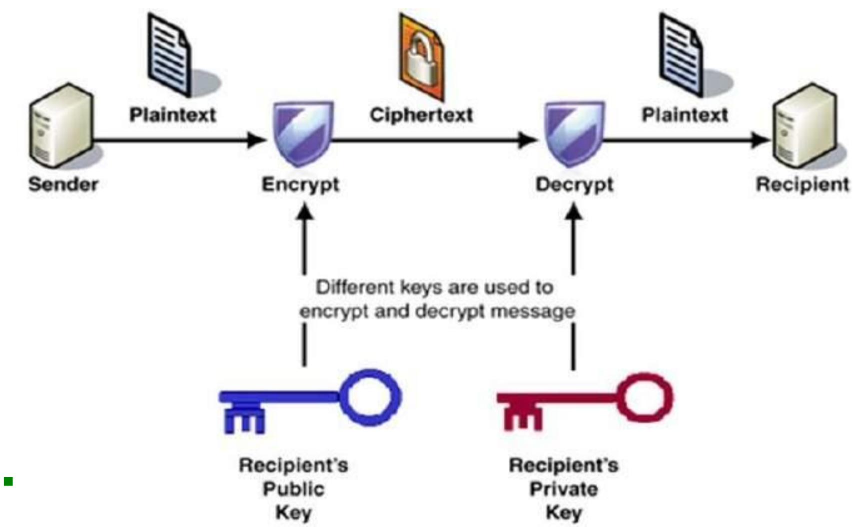
- **Factorize integer into primes** in **polynomial time**
  - Best classical algorithm: **subexponential**

    (but: **not NP-complete**)

$$\mathbf{21 = 3 \cdot 7}$$



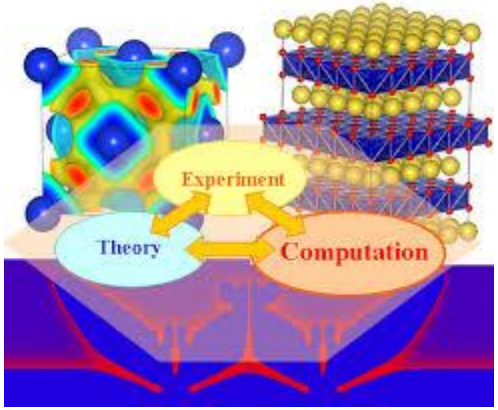
- **Break public key encryption** (**RSA**, …) **!**
  - use **quantum encryption**

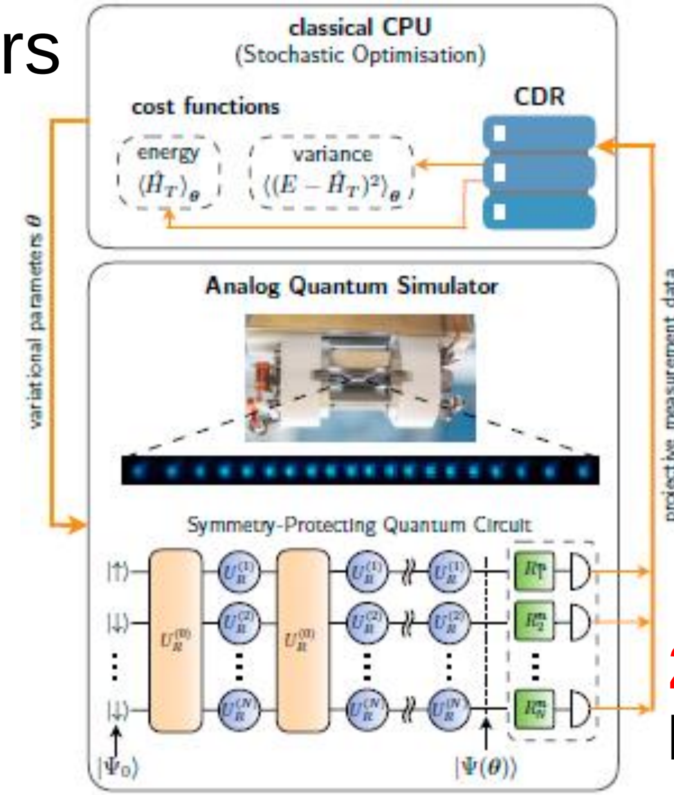


  - or **classical post-quantum …**

Materials Science

- **Variational** solvers



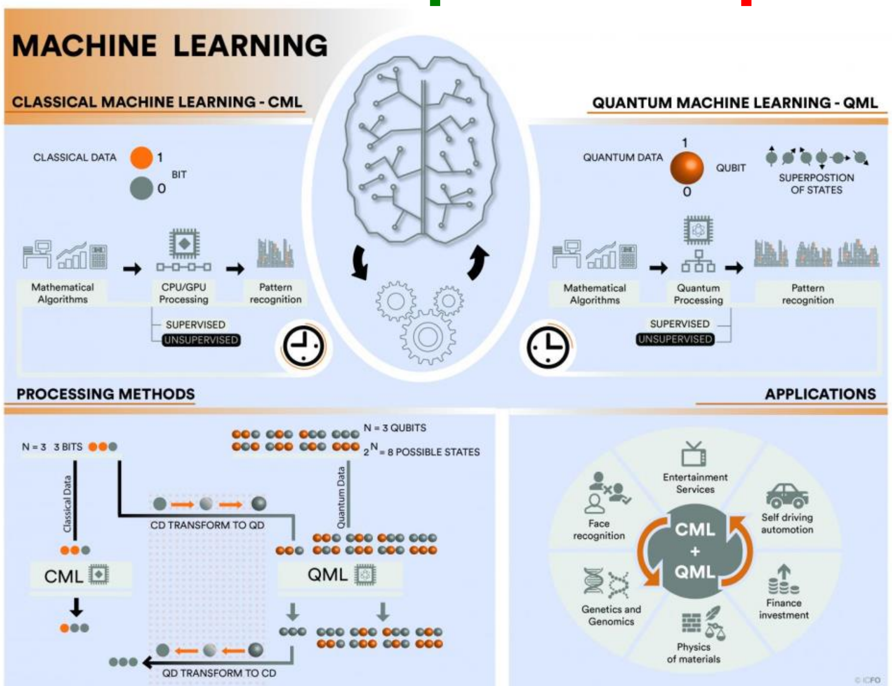


20 qubits
[Blatt-Roos-Zoller, 2018]

- **Full** solution:
  - **Classical**: **NP complete** (**2D**)
  - **Quantum**: **Quantum Merlin-Arthur** (**QMA**) **complete** (**1D**)

Quantum Machine Learning

- **Classical** vs. **quantum data**
- **Classical** vs. **quantum processing**

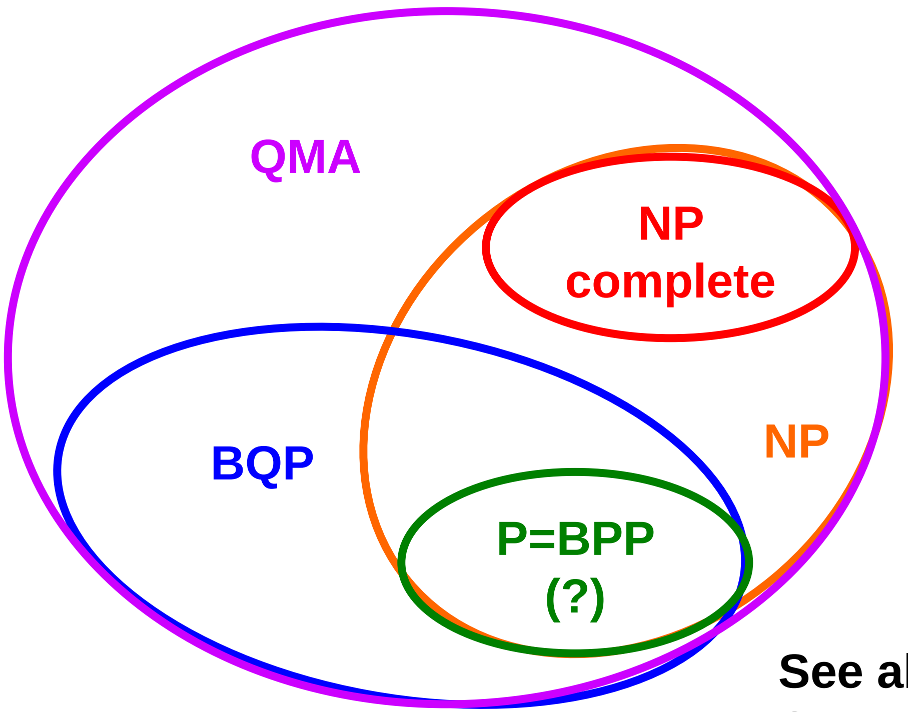


- Example of **caveats**:
  Quantum recommender

See also:
Scott Aaronson, *Read the Fine Print*

Quantum Complexity

- Best **indications**:
  - **QC cannot** solve **NP complete**
  - **QC can** solve problems outside **NP** (or **P-hierarchy**)



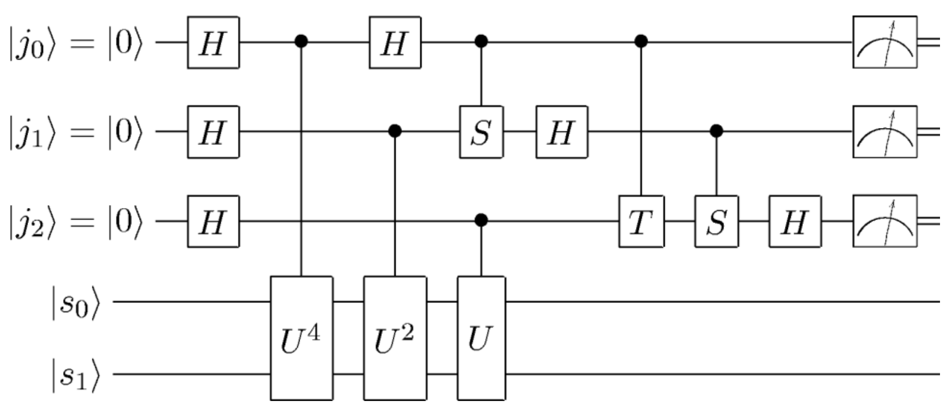
See also:
Scott Aaronson, *Quantum Computing since Democritus*

Outline

- Classical computation
- Quantum computation
  - The idea
  - Power & limitations
  - $\boxed{\text{– Architectures}}$

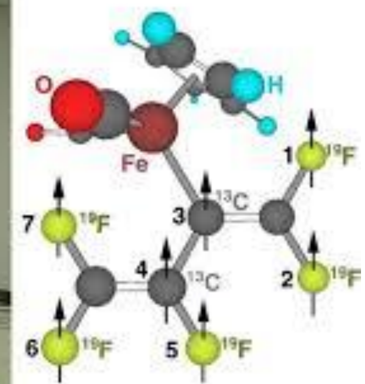
How to Build a QC?

- **DiVincenzo** criteria (**1996**)
  - **Scalable** well-defined **qubits**
  - **Initialization**
  - **Individual measurement**
  - **Universal gates**
  - Long **coherence times**

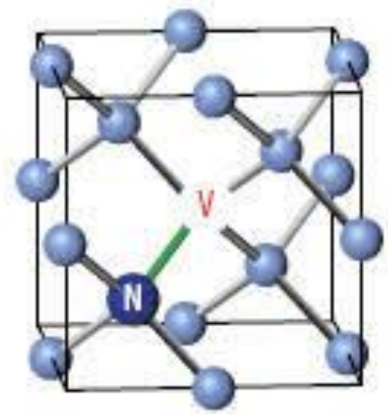


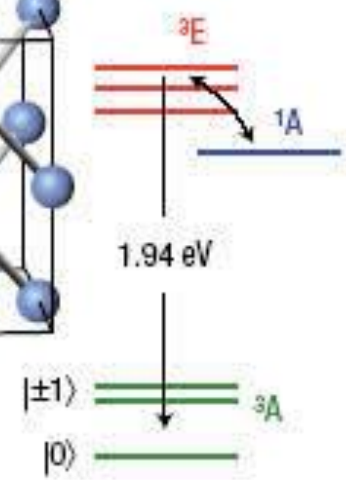
Spin QC

- **NMR**



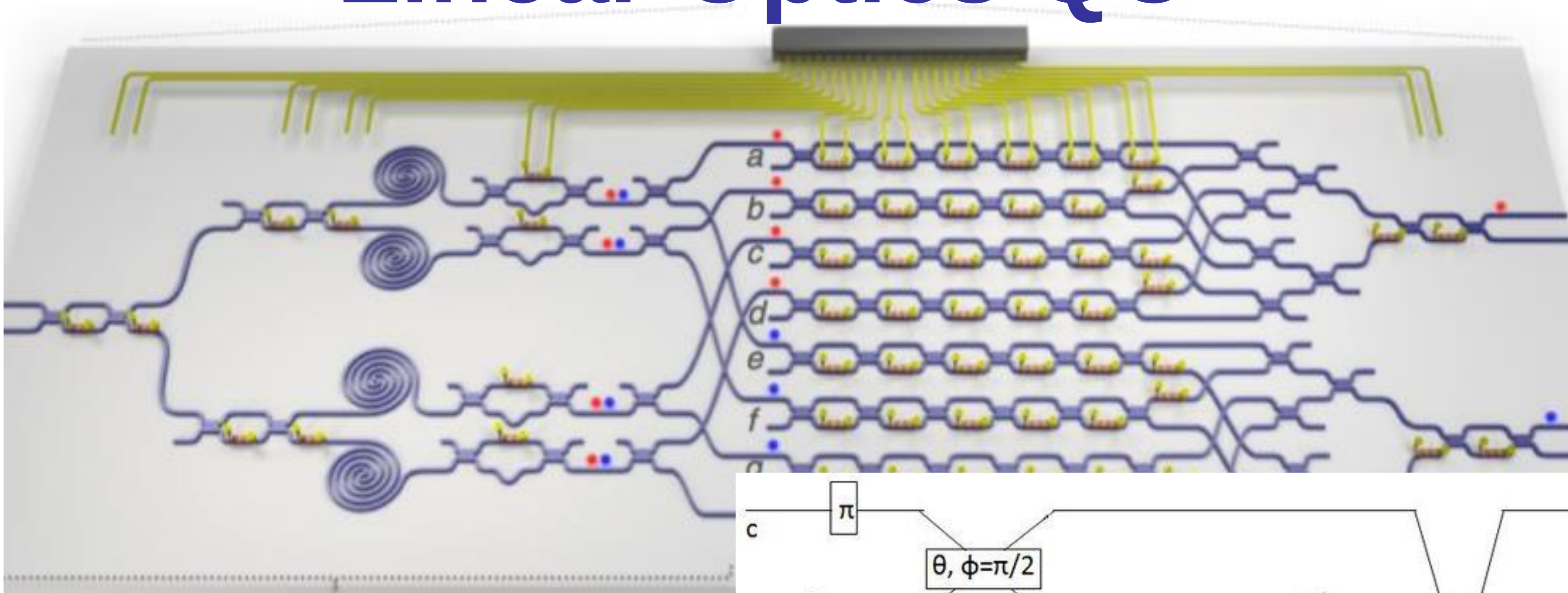
- **NV centers** in **diamond**

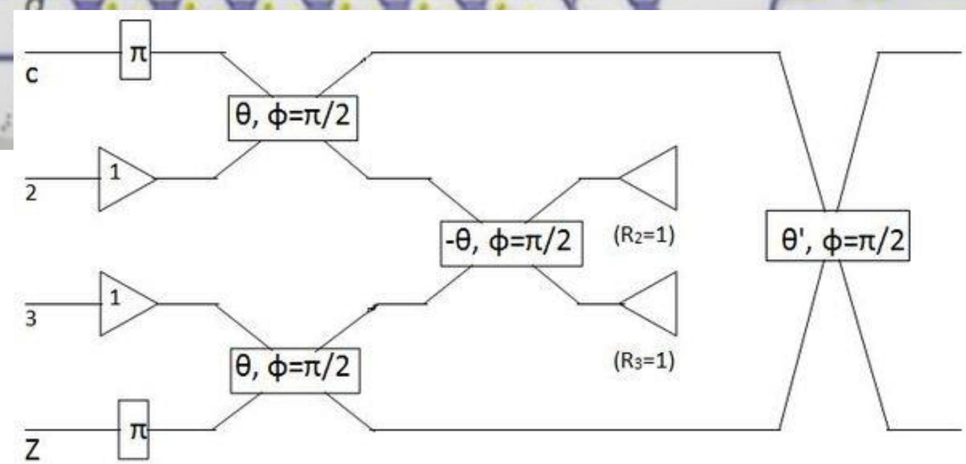




- **Good**: **coherence** (**room temperature !**)
- **Bad**: **2-qubit gates**, **scalability**

Linear Optics QC

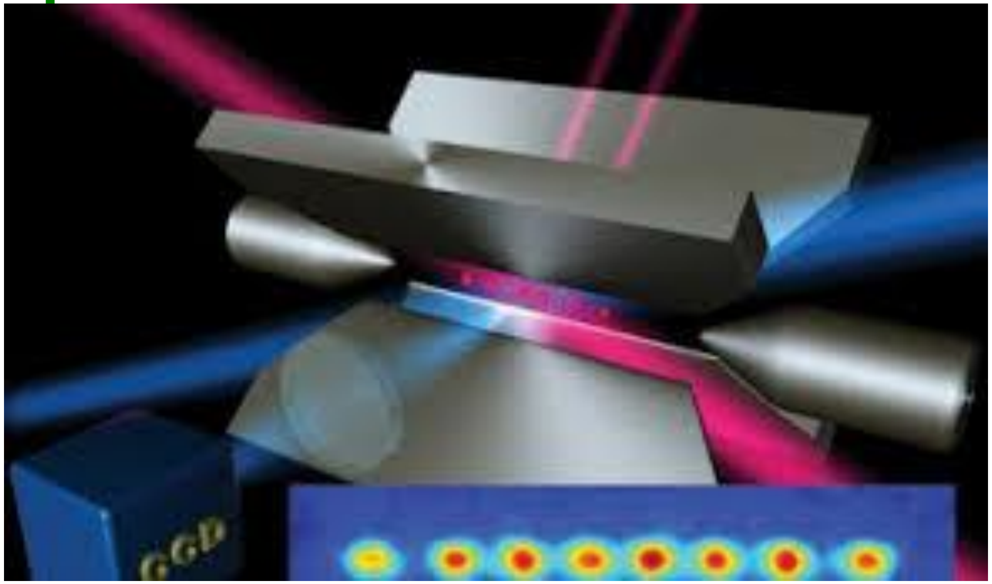




- **2-qubit**:
  - Linear + **measurement**
  - Could be **pre-prepared**
- **Good**: **coherence**, **scalability**
- **Bad**: **2-qubit gates**

Trapped Ions

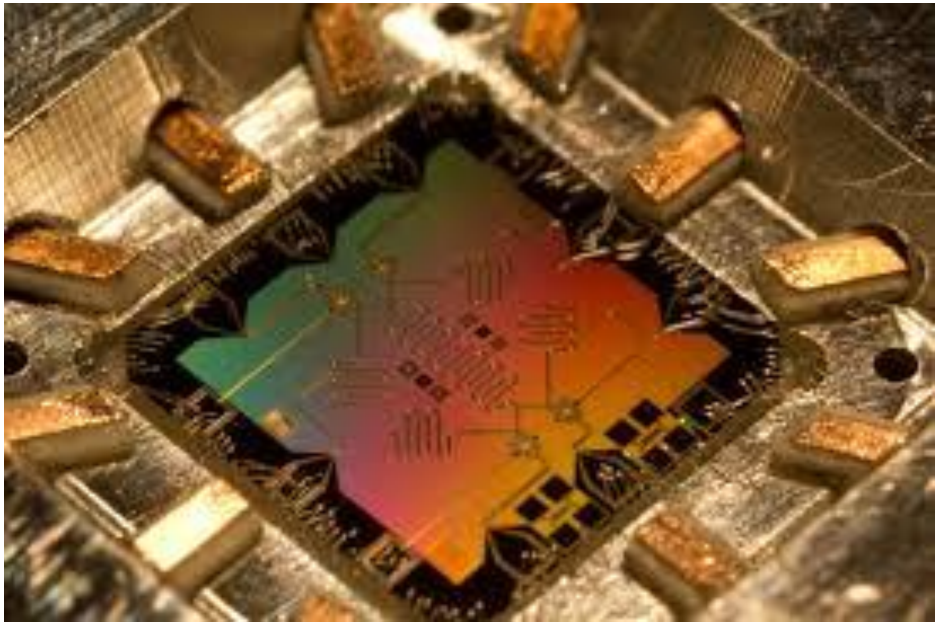
- **Cold** ($< 1\ \mu\mathrm{K}$) **ions** in **electromagntic trap**
  - **1-qubit gates**: **optical**
  - **2-qubit gates**: via **trap modes**

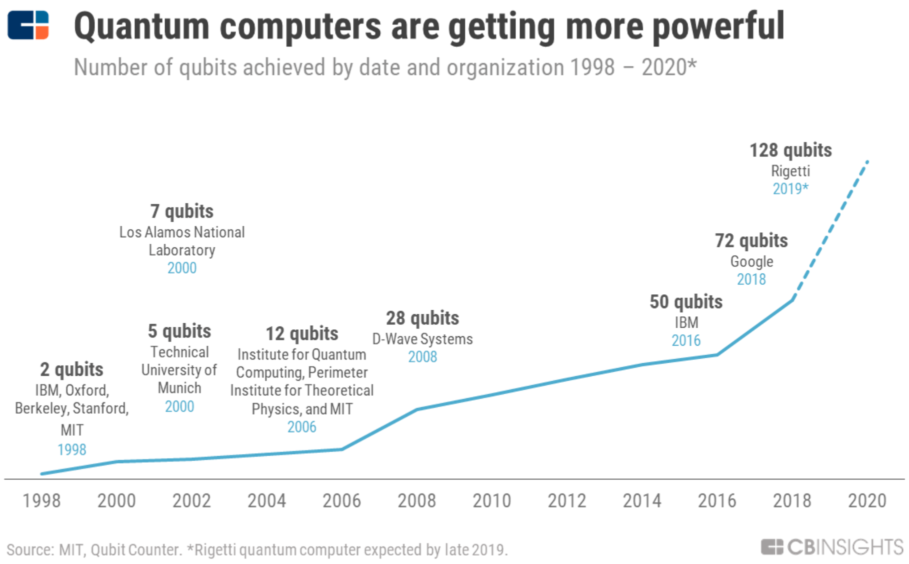


- **Scaling:**
  - **move ions**
  - via **photons**
- **Good**: **coherence**
- **Bad**: **scalability**

Superconducting

- Nonlinear quantum circuits
  - Josephson effect





- Good: scalability (>50 already!)
  - D-wave: 2000-qubit annealer
- Bad: uniformity, coherence

Quantum Error Correction

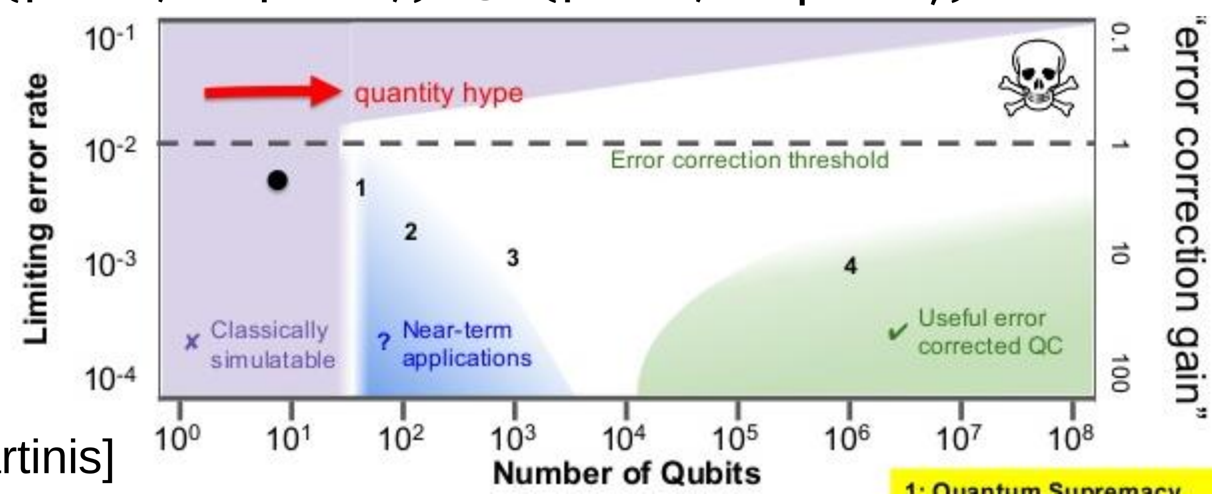
- **Classical error correction**: **1** ▶ **0**

  111 ▶ **101** ▶ **111**

- **Quantum error correction:**
  - **cannot measure !?**
  - **phase errors !?** $|\mathbf{111}\rangle$ ▶ $-|\mathbf{111}\rangle$
- Still possible **!**
  - Example (**Shor**): encode $|1\rangle, |0\rangle$ in **9** qubits

  $$(|\mathbf{111}\rangle \pm |\mathbf{000}\rangle) \otimes (|\mathbf{111}\rangle \pm |\mathbf{000}\rangle) \otimes (|\mathbf{111}\rangle \pm |\mathbf{000}\rangle)$$

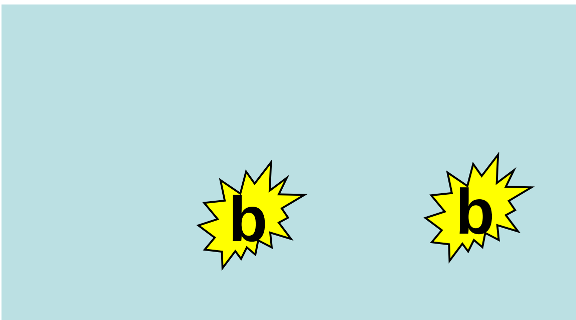
  - Error **threshold**



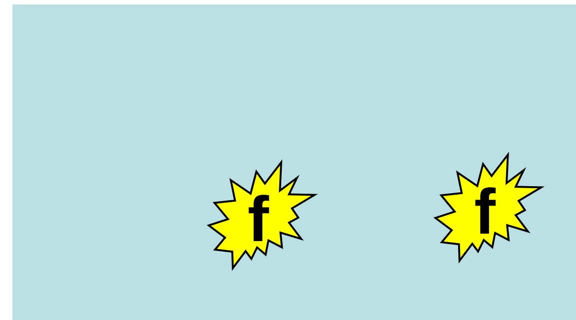
[Martinis]

Topological QC (I)

- **bosons vs. fermions**:

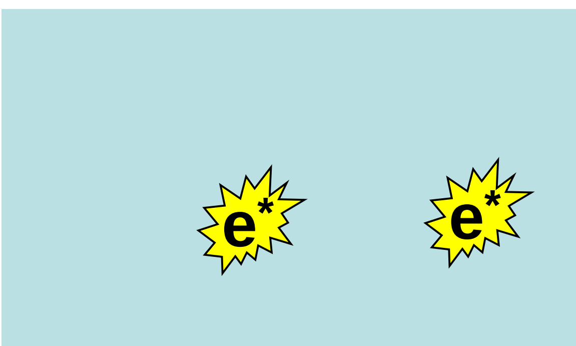


$$\psi_B(\mathbf{r}_1,\mathbf{r}_2) \to +\psi_B(\mathbf{r}_1,\mathbf{r}_2)$$



$$\psi_F(\mathbf{r}_1,\mathbf{r}_2) \to -\psi_F(\mathbf{r}_1,\mathbf{r}_2)$$

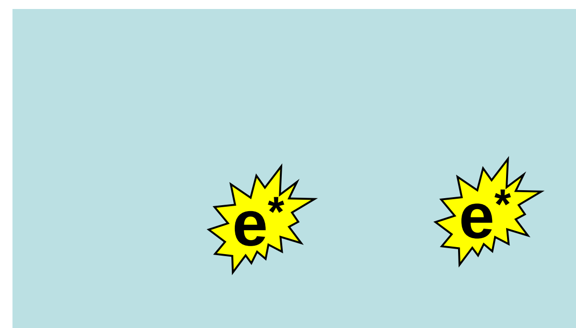
- **fractional excitations** (**fractional quantum Hall…**):



  – charge **e*** encircling a **flux quantum**

$$\psi_{e^*}(\mathbf{r}_1,\mathbf{r}_2) \to e^{2i\theta^*}\psi_{e^*}(\mathbf{r}_1,\mathbf{r}_2)$$

$$\theta^* = 2\pi(e^*/e)$$

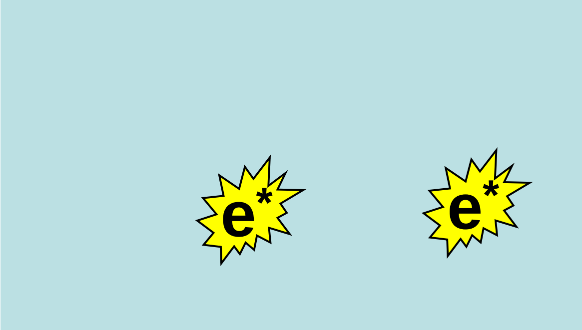


$$\psi_{e^*}(\mathbf{r}_1,\mathbf{r}_2) \to e^{i\theta^*}\psi_{e^*}(\mathbf{r}_1,\mathbf{r}_2)$$

  – **fractional statistics** (**anyons**)**!**

Topological QC (II)

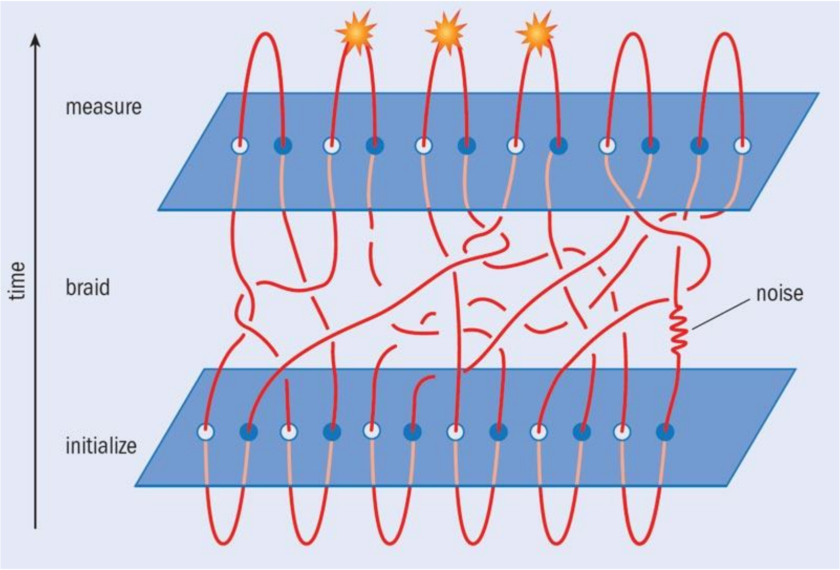
- If state of two anyons is **degenerate**: $\psi_{e^*,\mu}(\mathbf{r}_1,\mathbf{r}_2)$



$$\psi_{e^*,\mu}(\mathbf{r}_1,\mathbf{r}_2) \to \sum_\nu U_{\mu\nu} e^{i\theta^*} \psi_{e^*,\nu}(\mathbf{r}_1,\mathbf{r}_2)$$

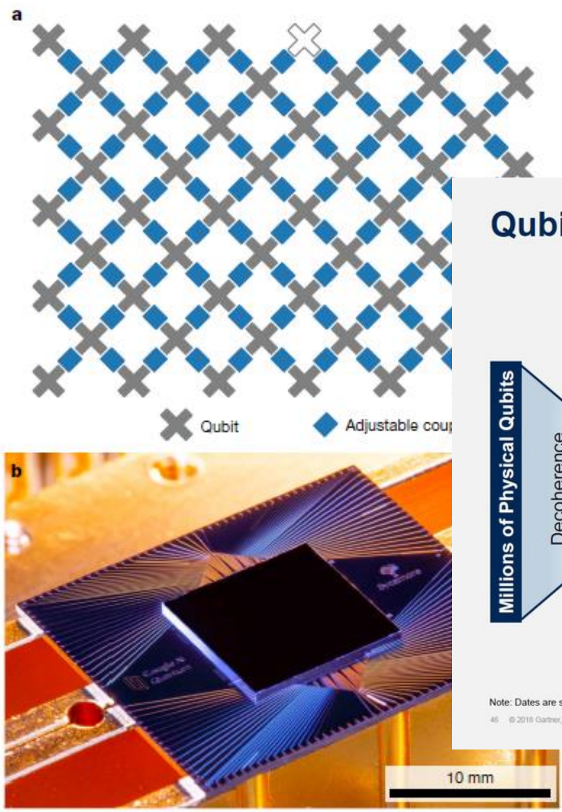
– **non-abelian statistics!**

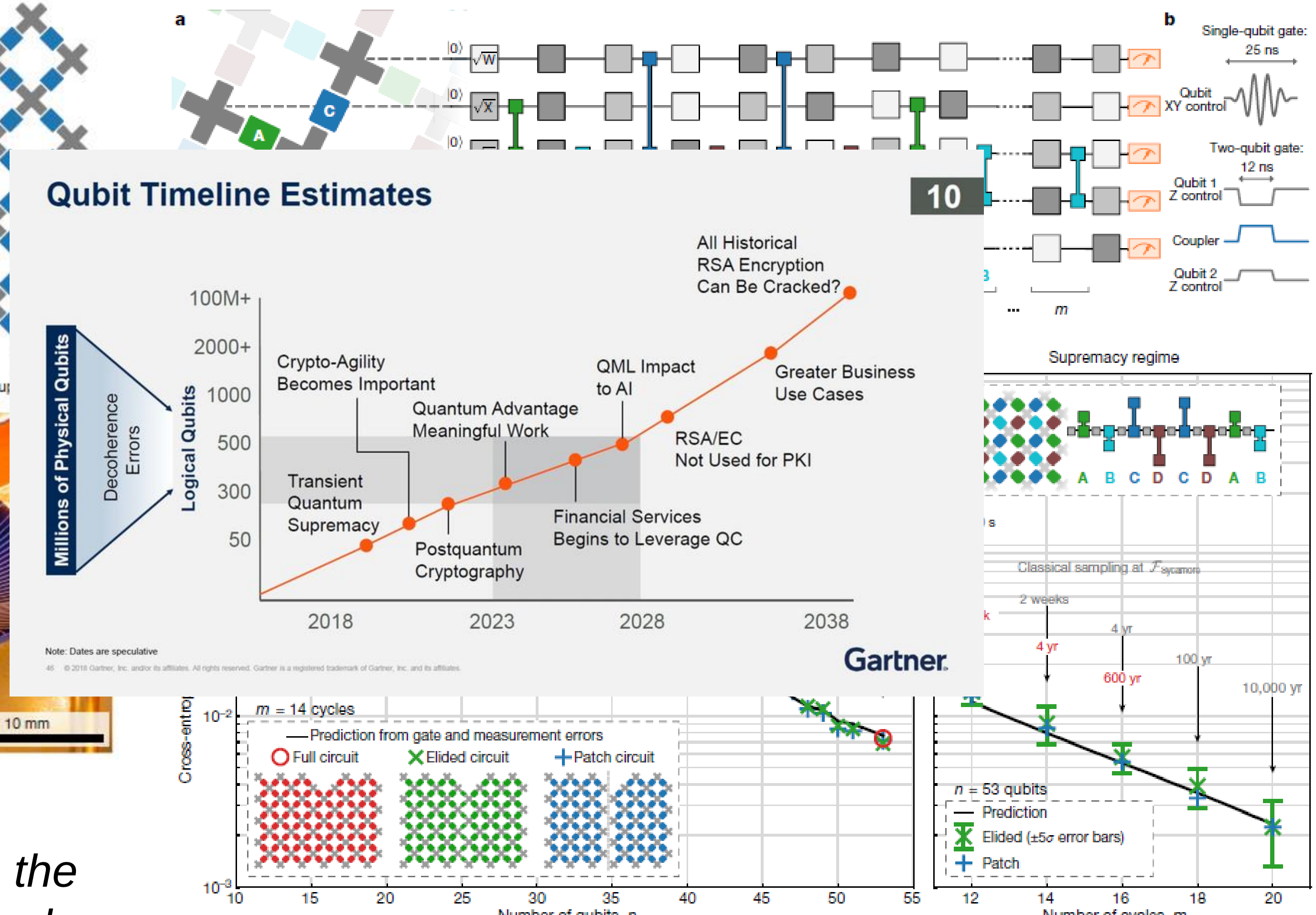
- **topological quantum computation**:



The Next Steps?

- Noisy Intermediate Scale Quantum (**NISQ**):
  - **Quantum supremacy**: **beyond best classical computer**





See also:
John Preskill, *QC in the NISQ Era and Beyond*


HOW'S YOUR QUANTUM COMPUTER PROTOTYPE COMING ALONG?
GREAT!
THE PROJECT EXISTS IN A SIMULTANEOUS STATE OF BEING BOTH TOTALLY SUCCESSFUL AND NOT EVEN STARTED.
CAN I OBSERVE IT?
THAT'S A TRICKY QUESTION.
Dilbert.com
DilbertCartoonist@gmail.com
4-7-12 © 2012 Scott Adams, Inc.

Thank You!