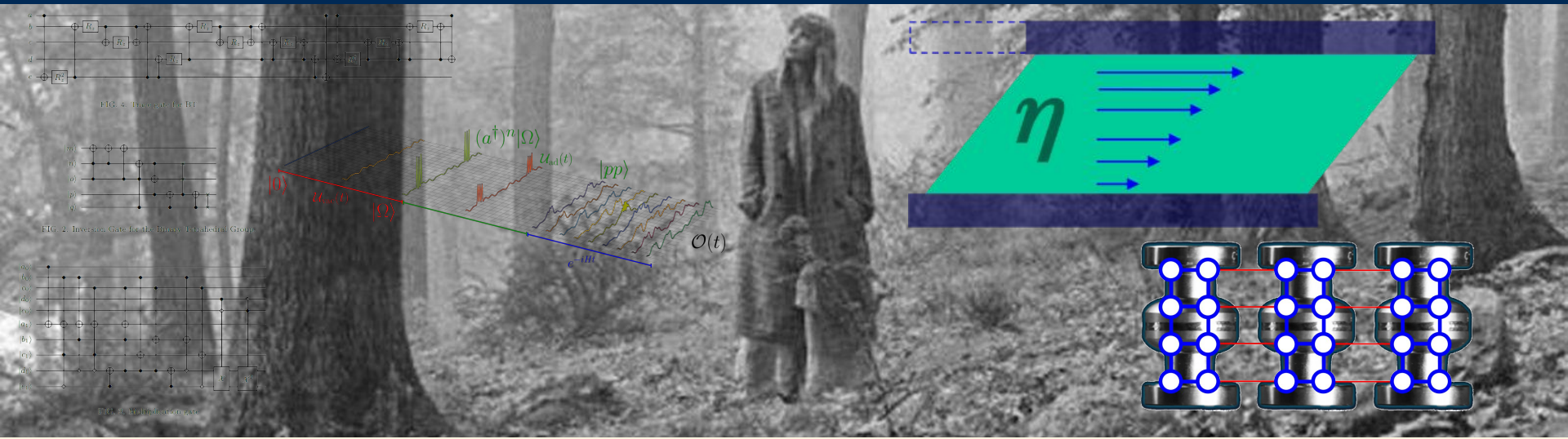
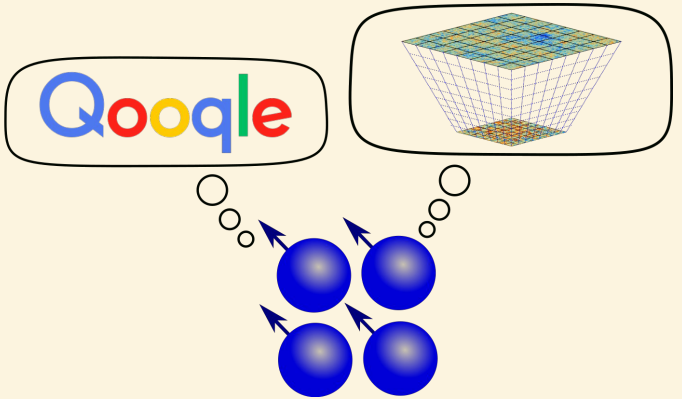


Introduction to Quantum Computing

Hank Lamm
Theory Division

July 13, 2023



Lots of Interest, Lots of Hype, Lots of $$

FUNDING SECURED

CONGRESS PASSES $1.2 BILLION QUANTUM COMPUTING BILL

NEURAL

Quantum Computing Quantum News

How quantum computers could make future humans immortal

Quantum Computing: The Potential Cure For Cancer?

Pete Tseronis April 25, 2018

'QUANTUM APOCALYPSE': HOW ULTRA-POWERFUL COMPUTERS COULD CRIPPLE GOVERNMENTS AND EFFECTIVELY BREAK THE INTERNET

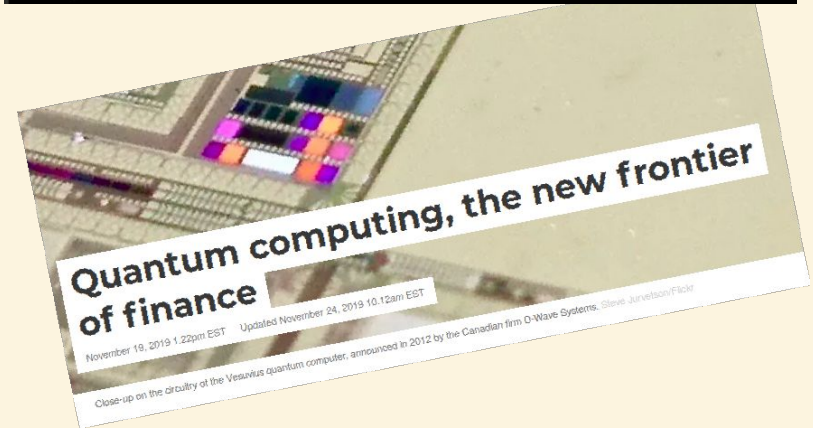
'Our modern systems of finance, commerce, communication, government, and healthcare will for all intents and

Quantum computers could slash the energy use of cryptocurrencies

Mining cryptocurrencies like bitcoin could be done using quantum computers, cutting their electricity use by 90 per cent

By Alex Wilkins

20 June 2023



Quantum computing, the new frontier of finance

November 19, 2019 1.22pm EST Updated November 24, 2019 10.12am EST

Close-up on the circuitry of the Vesuvius quantum computer, announced in 2012 by the Canadian firm D-Wave Systems. Steve Jurvetson/Flickr

Lots of Interest, Lots of Hype, Lots of $$

So, today I hope to answer one question

…which is really a bunch of smaller questions

- What is **wrong** with classical computing?
- How do **quantum computers** work?
- What **can I do** today?
- What does the **future** look like?

Who am I?

Physics PhD at

Physics/Mech&Nuke Eng Undergrad at KANSAS STATE UNIVERSITY

Nuclear Theory Postdoc at UNIVERSITY OF MARYLAND

Arizona State University

HEP Theory Postdoc -> Associate Scientist at Fermilab

What do I do?

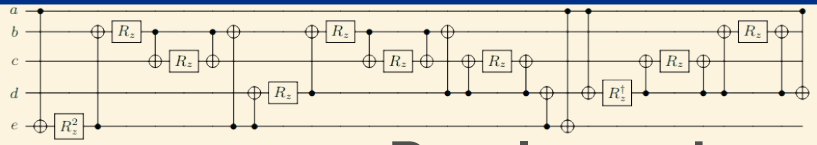


FIG. 4. Trace gate for BT

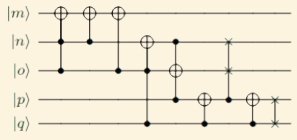


FIG. 2. Inversion Gate for the Binary Tetrahedral Group.

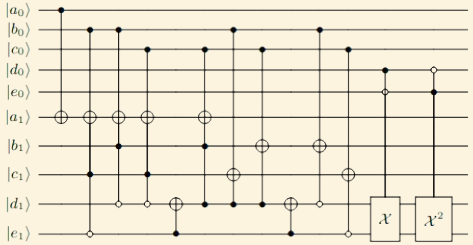


FIG. 3. Multiplication gate

Develop and apply quantum computing to solve problems in high energy physics

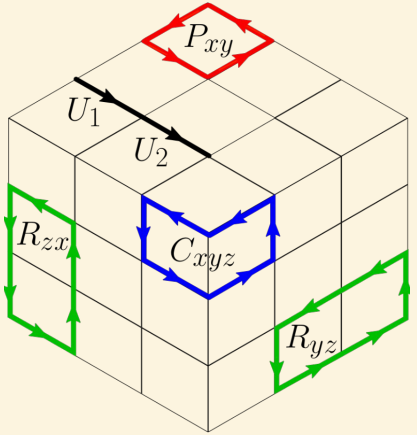
Does the **universe's expansion** affect phase transitions?

How does the **viscosity** of the QGP manifest in particle collisions?

Can we formulate **lattice field theory** for quantum computers?

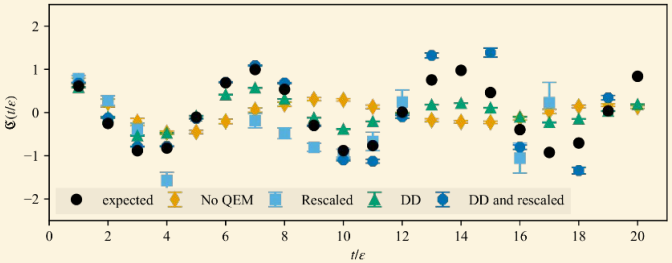
What **gate set and hardware** is necessary for simulating physics?

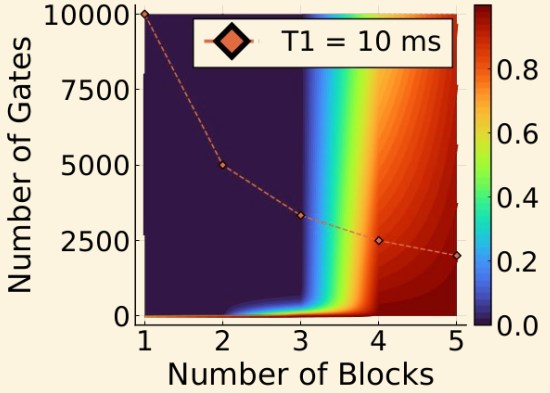
Is **error mitigation** able to extend the reach of QC?



Sit behind a computer and write code

Stand at a blackboard and have long conversations





What makes a classical computer?

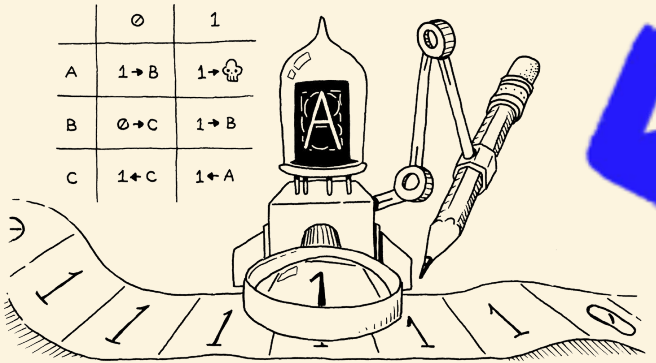

```php
$mail->setFrom('from@example.com', 'Mailer');
$mail->addAddress('joe@example.net', 'Joe User');     // Add a recipient
$mail->addAddress('ellen@example.com');               // Name is optional
$mail->addReplyTo('info@example.com', 'Information');
$mail->addCC('cc@example.com');
$mail->addBCC('bcc@example.com');

$mail->addAttachment('/var/tmp/file.tar.gz');         // Add attachments
$mail->addAttachment('/tmp/image.jpg', 'new.jpg');    // Optional name
$mail->isHTML(true);                                  // Set email format to
HTML

$mail->Subject = 'Here is the subject';
$mail->Body    = 'This is the HTML message body <b>in bold!</b>';
$mail->AltBody = 'This is the body in plain text for non-HTML mail clients';

if(!$mail->send()) {
 echo 'Message could not be sent.';
 echo 'Mailer Error: ' . $mail->ErrorInfo;
} else {
 echo 'Message has been sent';
}
?>
```

Universal Turing Machine



- “Infinite” tape specifying a states
  - Usually in binary i.e. {0,1}
- CPU performs operations
  - Finite set of operations allow **any** classical computation

What does a classical computer do?

- ***algorithm (n):*** a set of rules to be followed in calculations

- **Problem:** Sort a list of numbers
- Algorithmic Solutions:
  - *Random:* Rearrange at random all numbers
  - *Bubble sort:* Compare switch pairwise
  - *QuickSort:* Sort elements about pivot

$$\begin{pmatrix} 13 & 63 & 14 \\ 68 & 52 & 30 \\ 59 & 56 & 73 \\ 4 & 54 & 32 \\ 17 & 6 & 23 \\ 47 & 96 & 38 \\ 50 & 59 & 72 \\ 39 & 64 & 44 \\ 71 & 39 & 51 \\ 85 & 6 & 11 \\ 20 & 49 & 84 \\ 46 & 62 & 68 \\ 61 & 17 & 4 \\ 41 & 77 & 83 \\ 64 & 21 & 7 \end{pmatrix}$$

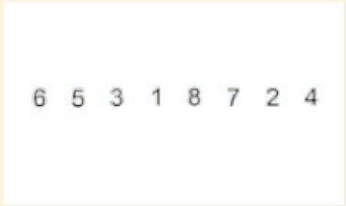
How about a visual demonstration?

How do algorithms differ? Complexity!

- **Time complexity:** How long will it take?
- **Space complexity:** How much memory does it take?
- **Big O notation:** Asymptotic behavior as a function of the size of the array, n

- **Bubble**
  $O(n^2)$

- **Insertion**
  $O(n^2)$

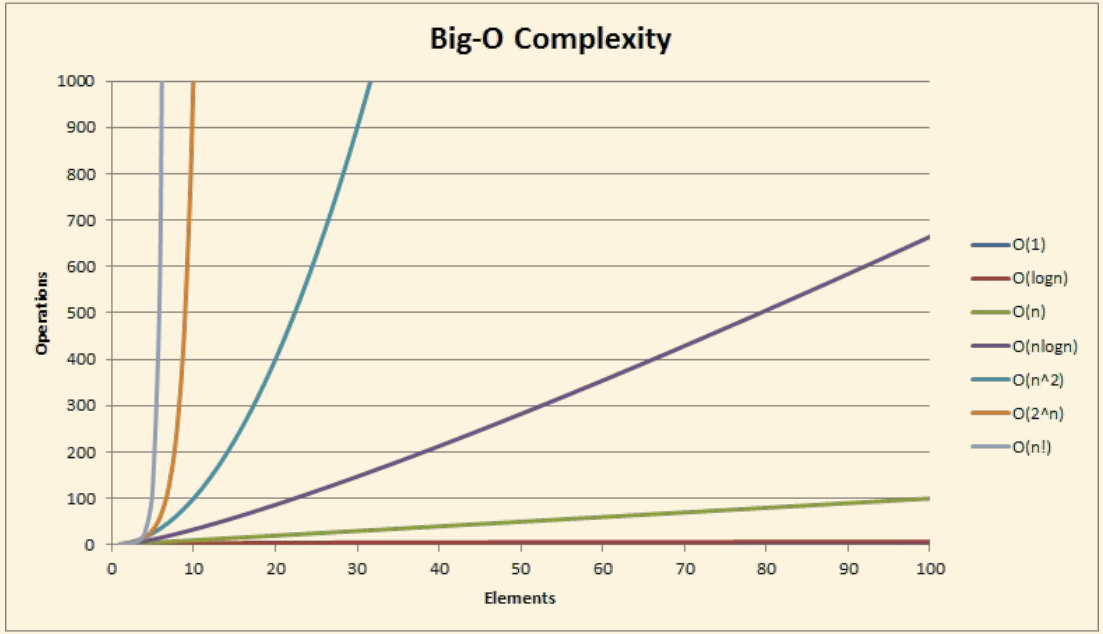


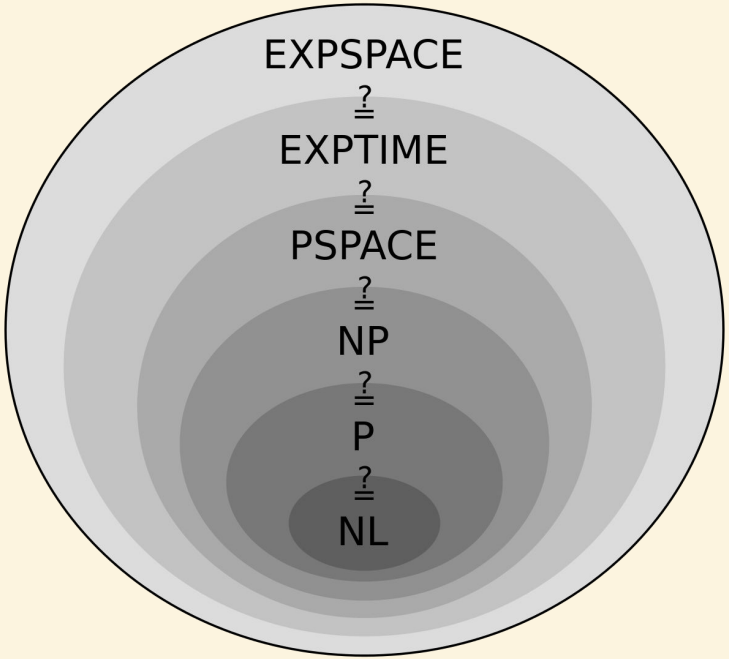
- **QuickSort**
  $O(n \log n)$

What's wrong with classical computing?

Problems can be classified by their complexity

Big-O Complexity Chart





https://github.com/gibsjose/cpp-cheat-sheet

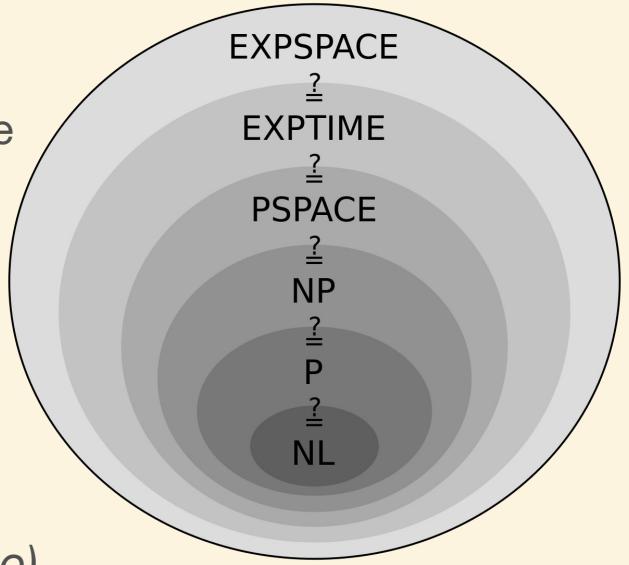
P vs. NP

- **P: Polynomial time problems**
  - number of operations that scale with the size like a power i.e. $O(n^2)$

- **NP: Nondeterministic polynomial time problems:**
  - correctness of solution is checkable in polynomial time
  - best deterministic algorithm scales faster i.e. $O(2^n)$

- Supercomputing resources are required to solving NP problems **for even smallish n**

- **Is P=NP?** Answer is worth a million dollars (*and fame*)



How the internet depends on complexity

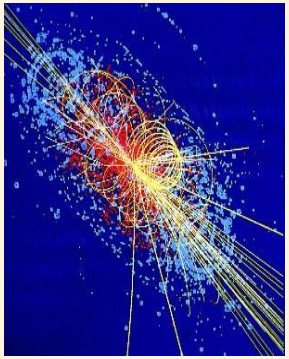
- **RSA encryption** is used to communicate online
- Based on **Prime Factorization**, **hoped** to be in NP
- **Best** known algorithm:

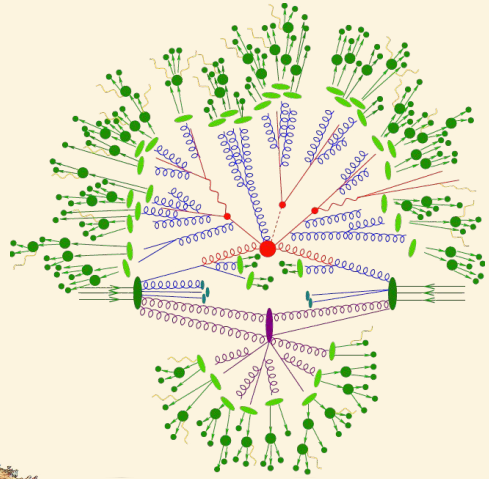
$$\exp\left(\left(\sqrt[3]{\frac{64}{9}}+o(1)\right)(\ln n)^{\frac{1}{3}}(\ln\ln n)^{\frac{2}{3}}\right)$$

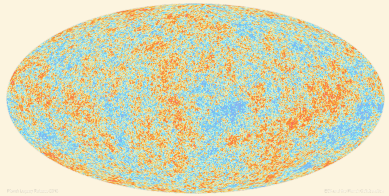
If we woke up to algo in P→ Chaos

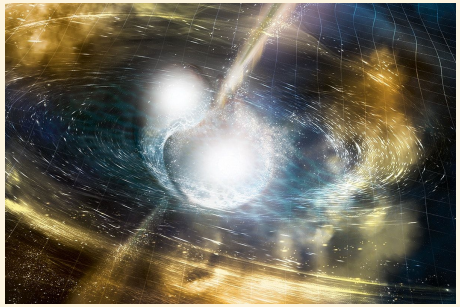
Why does physics struggle with NP…

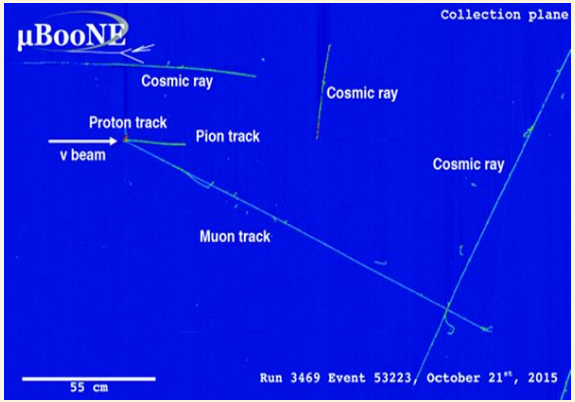
The world being quantum **literally** causes certain problems to have high computational complexity

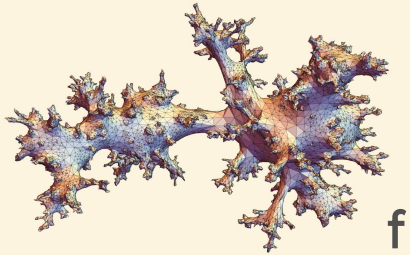


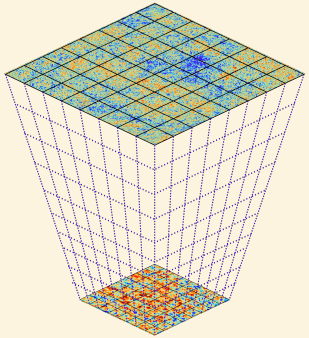












Nearly **any** hard problem in real time or finite density is believed to be at least NP.

…This is how nature works

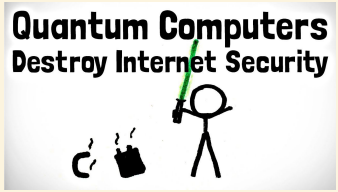
Classical computers are great as simulate classical processes

But nature is fundamentally quantum…

so I need a quantum computer to efficiently simulate it

What could a quantum computer do someday?

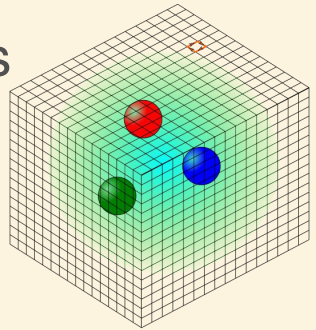
- **Shor's Algorithm** efficiently factorize
  - This is why people freak out!



- **Grover's Algorithm** efficiently perform searches

Qooqle

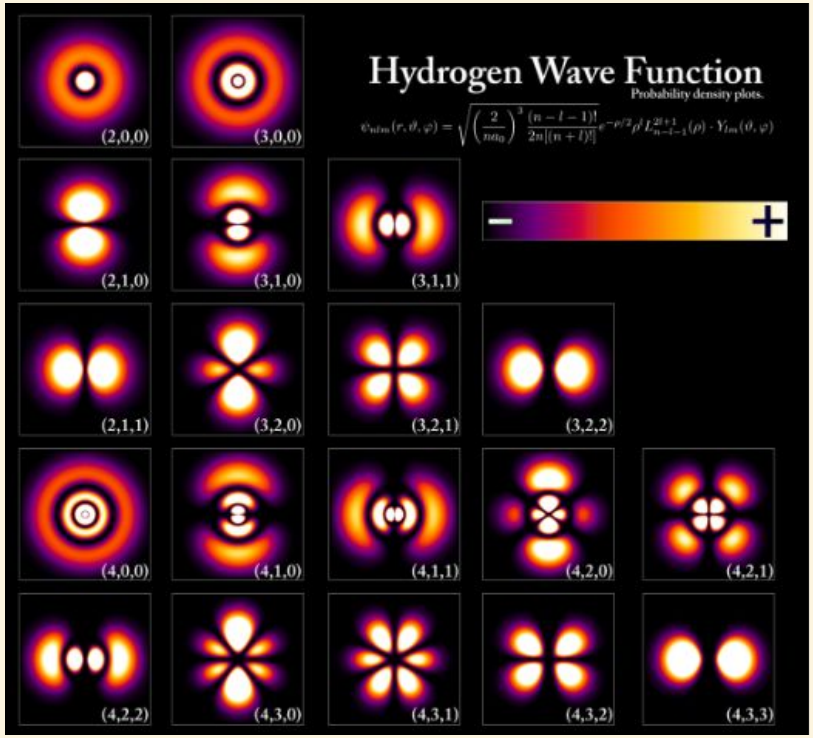
- Quantum Physics for Medicine and Materials
- High Energy Particle Physics *(Me!)*

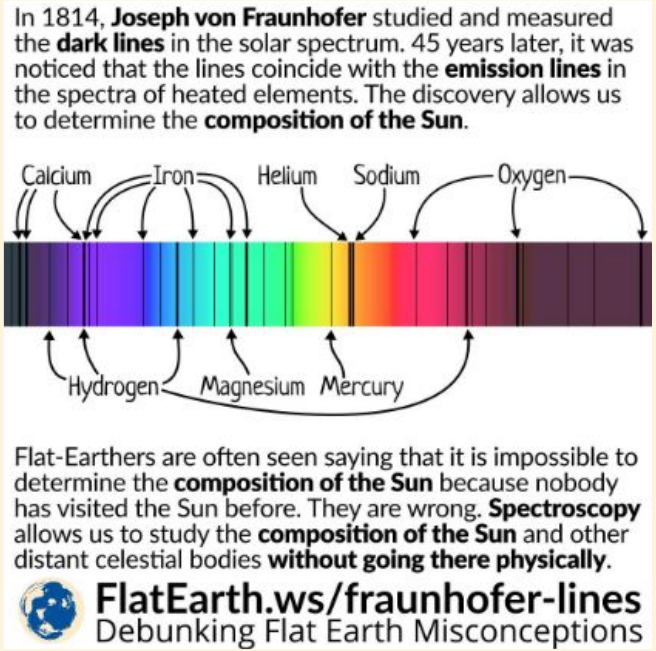


Not all problems have a faster quantum algorithm

Can't sorting faster

What's special about quantum mechanics? The quantum

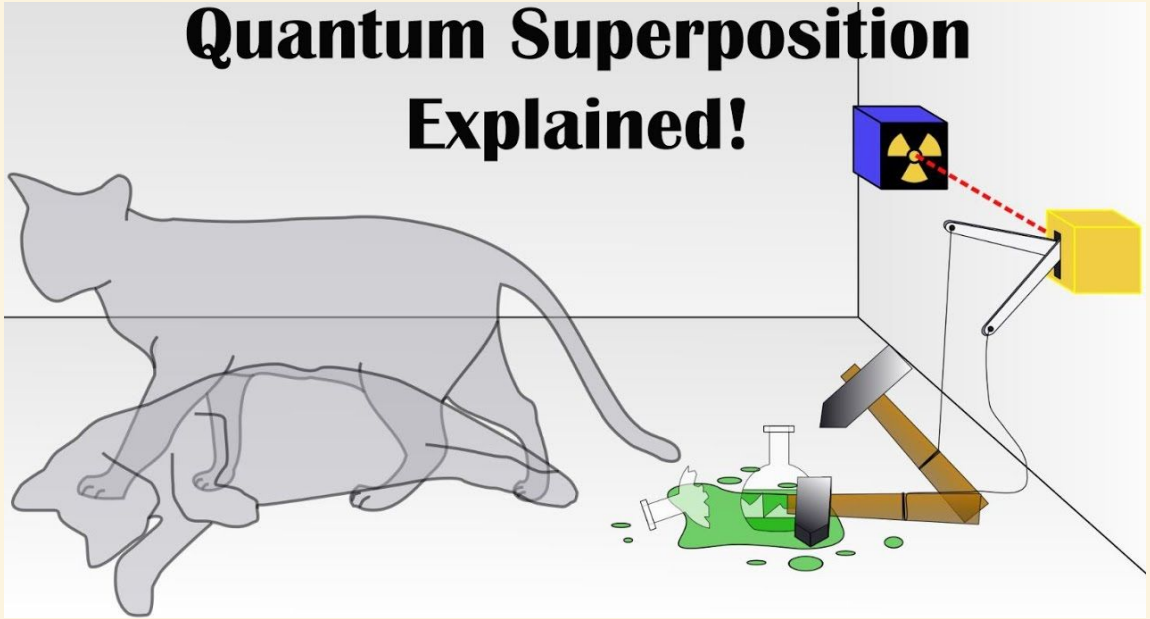




Quantized states: Only **specific values** of properties (e.g. energy) are allowed

What's special about quantum mechanics? Superposition!

Superposition: Systems can be in multiple states at once!



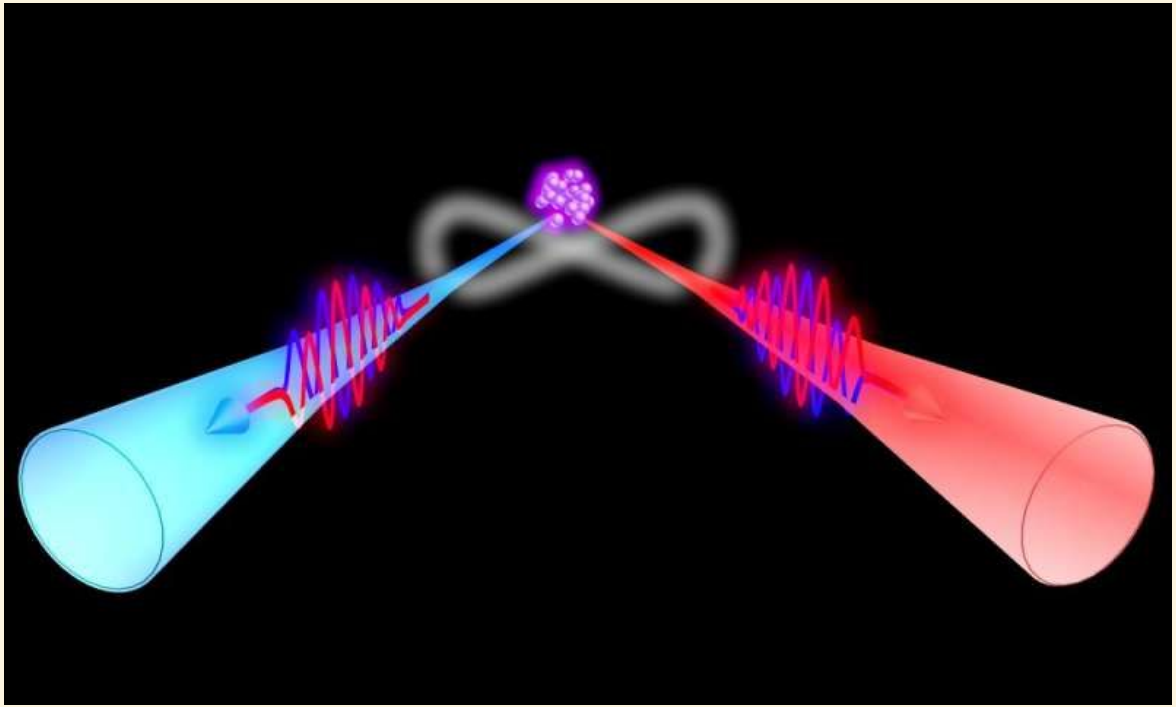
Wave function is sum

$|\Psi\rangle = a|\Psi_a\rangle + b|\Psi_b\rangle$

Upon measuring, $|\Psi\rangle$ ***"collapses"*** to a single state with probability e.g. $|a|^2$

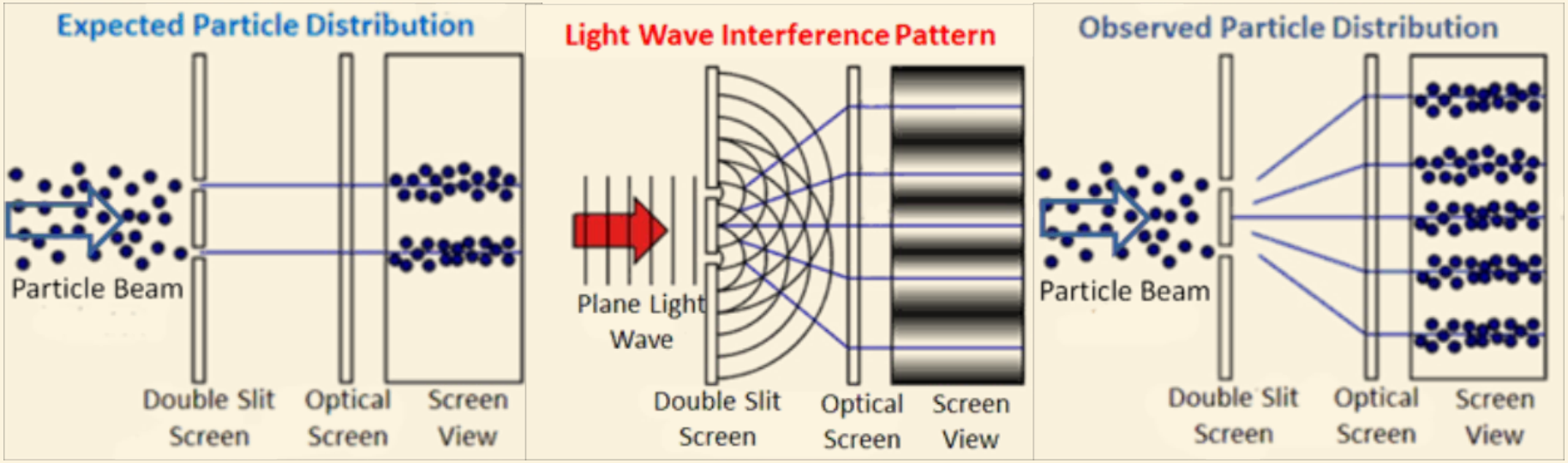
What's special about quantum mechanics? Entanglement!

Entanglement: States can't be subdivided into single particle states



Spooky action at a distance!

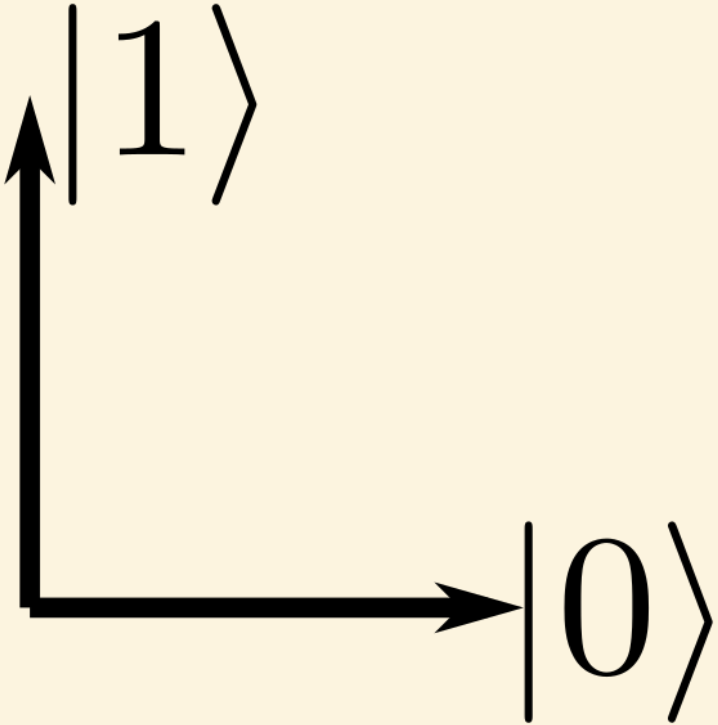
What's special about quantum mechanics? Interference!



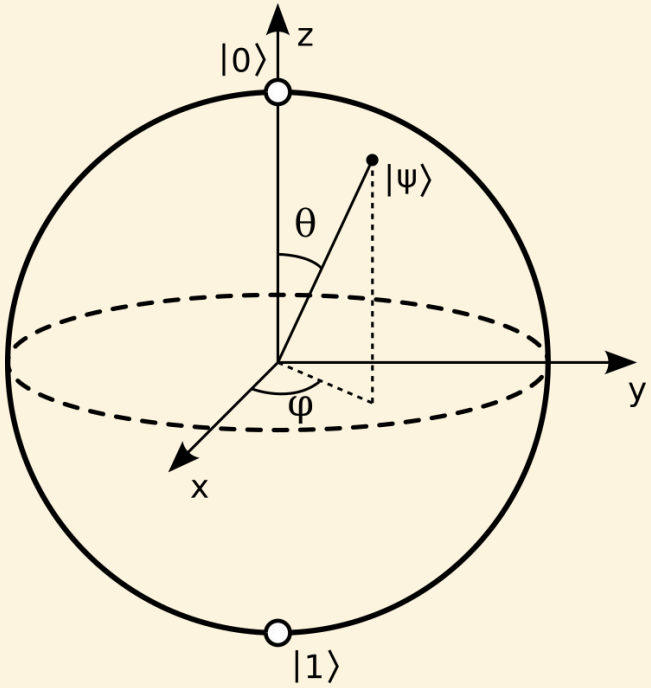
Particle-wave duality: a "particle" behaves in wave-like ways, such as interfering with itself; a "wave" behaves in particle like waves, such as point-like collisions

How does a qubit differ from classical bit?

Bit = {0,1}

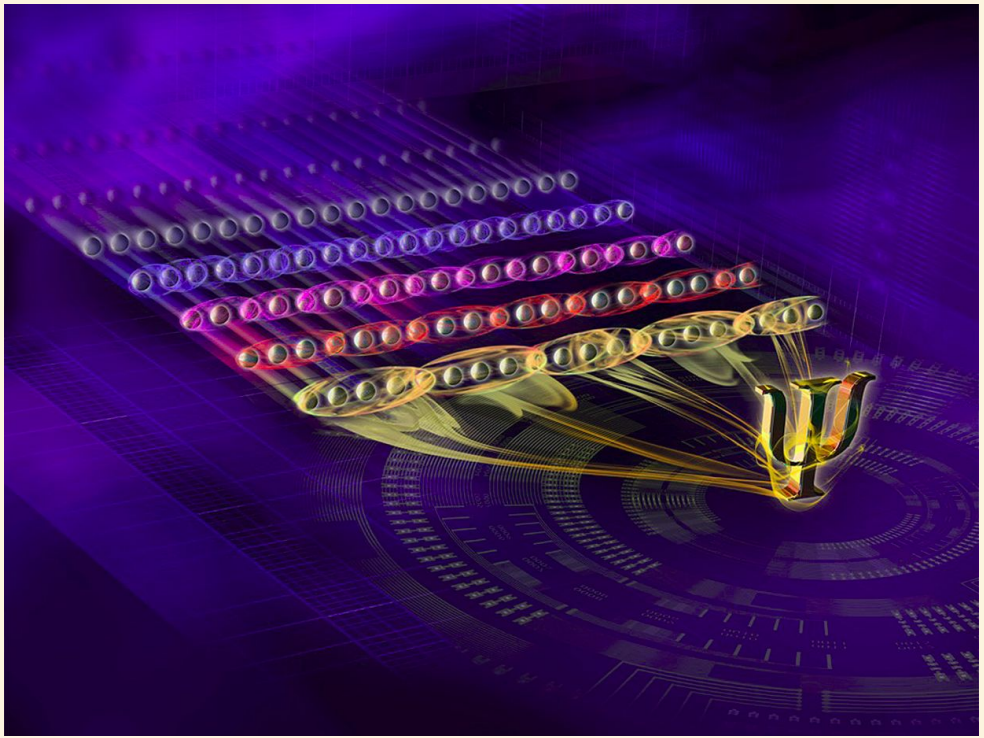


Qubit = a|0>+b|1>, a superposition!



How does a set of qubits differ from bits?

Bits = {0,1}x{0,1}={00,01,10,11}



Qubits = a|00>+b|01>+c|10>+d|11>, **superpositions and entangled!**

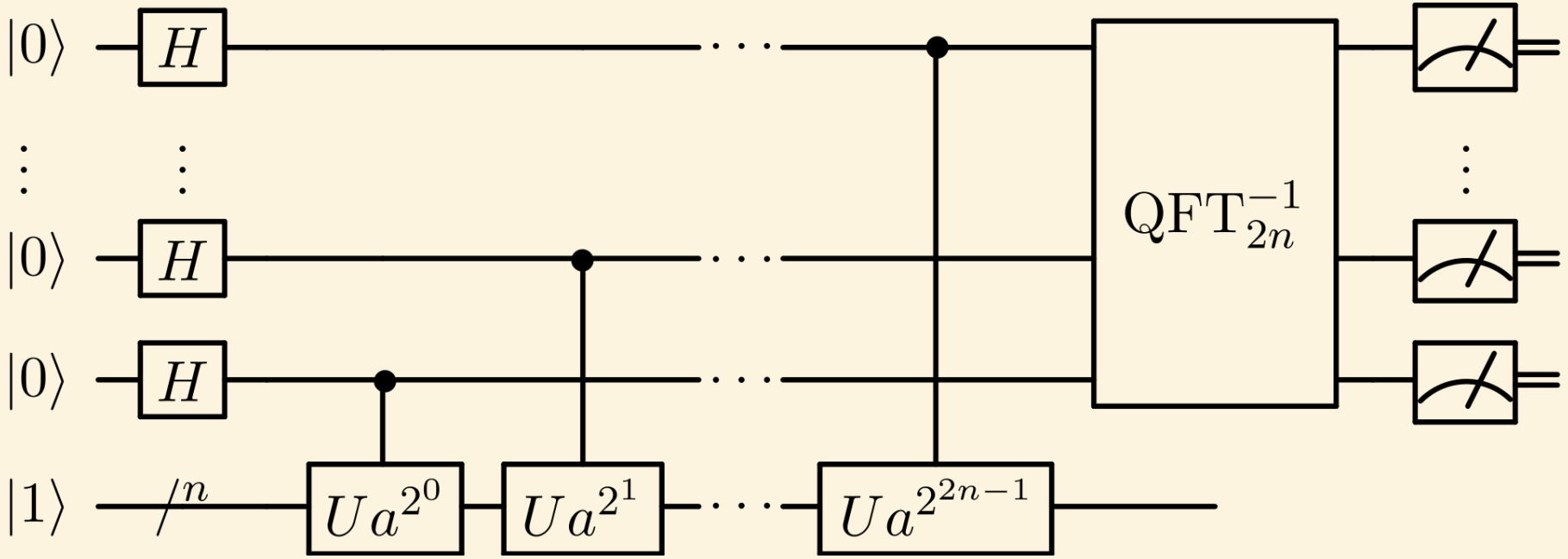
The basics of Quantum Information: Qubit storage

- For **n** qubits, there are 2^n amplitudes
- Need 2^n complex numbers for $|\Psi\rangle$
- Sycamore (53 qubits) need 1 PB
  - **Human brain** ~ 3 PB
  - **Summit at Oak Ridge** ~ 10 PB

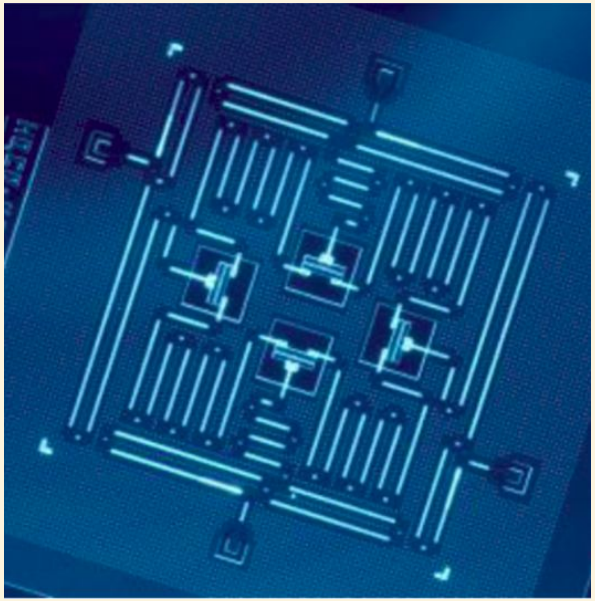
But, for small **n**<20, we can **classically** simulate the QC on a laptop.
This is super useful for algorithm research!

Basics of quantum algorithms

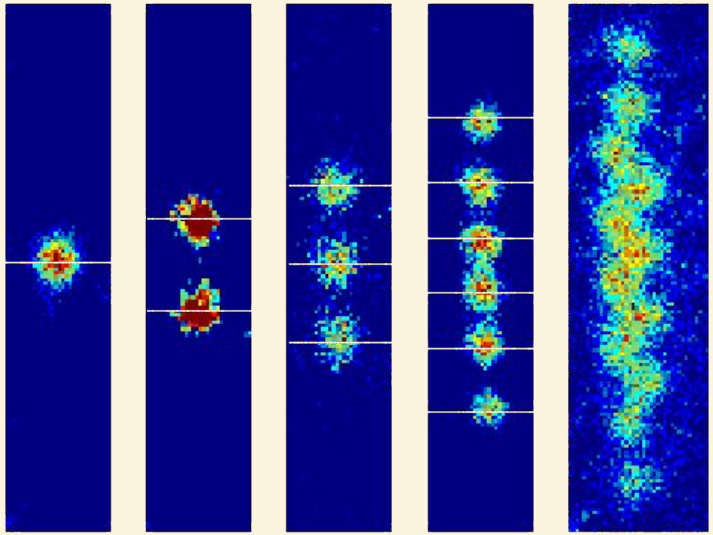
Prepare state → Apply gates → Measure probabilities



What are they made from?



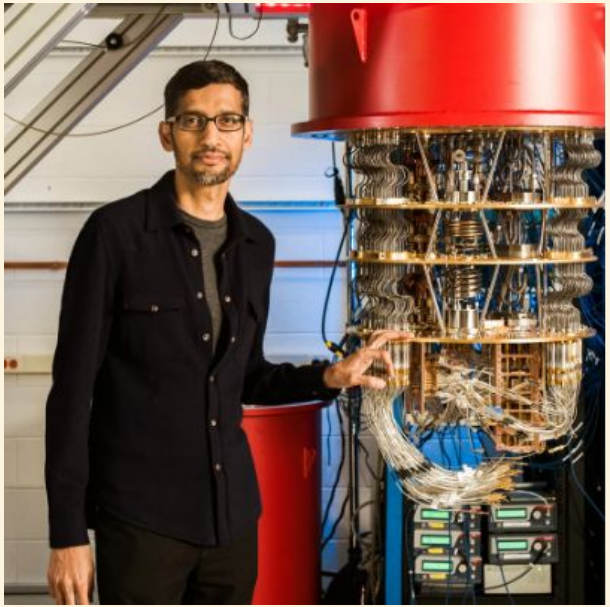
Microchips



Cold Ions/Atoms

Cavities

What do they look like?

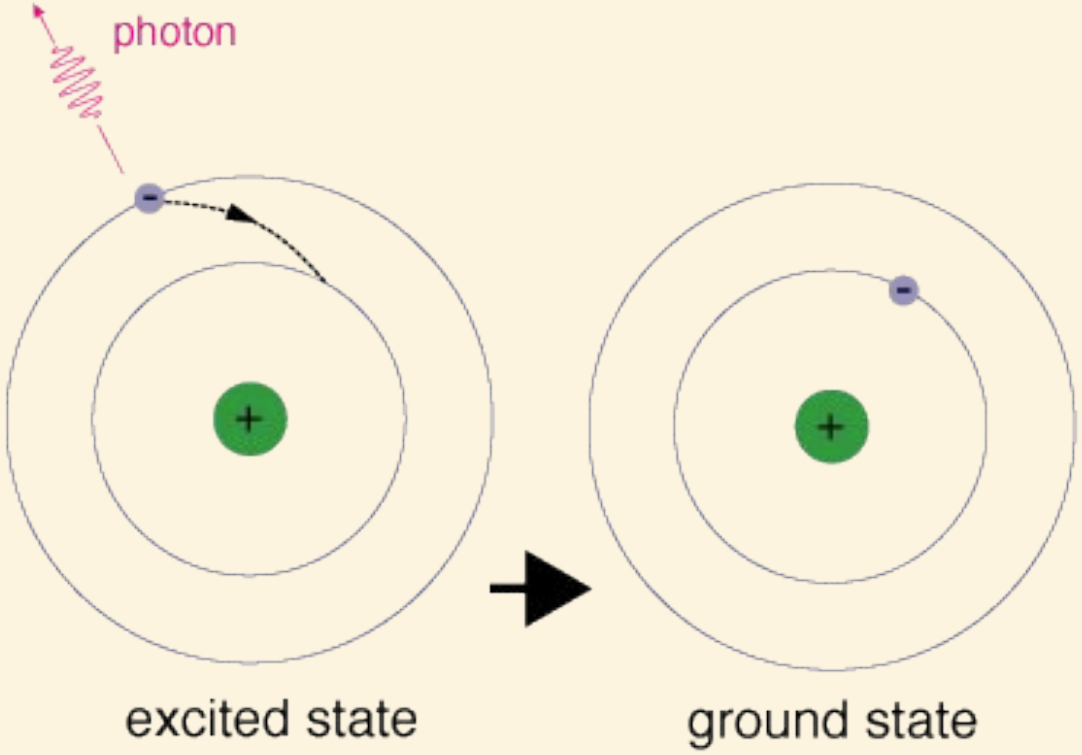


On site you can see some

SQMS!

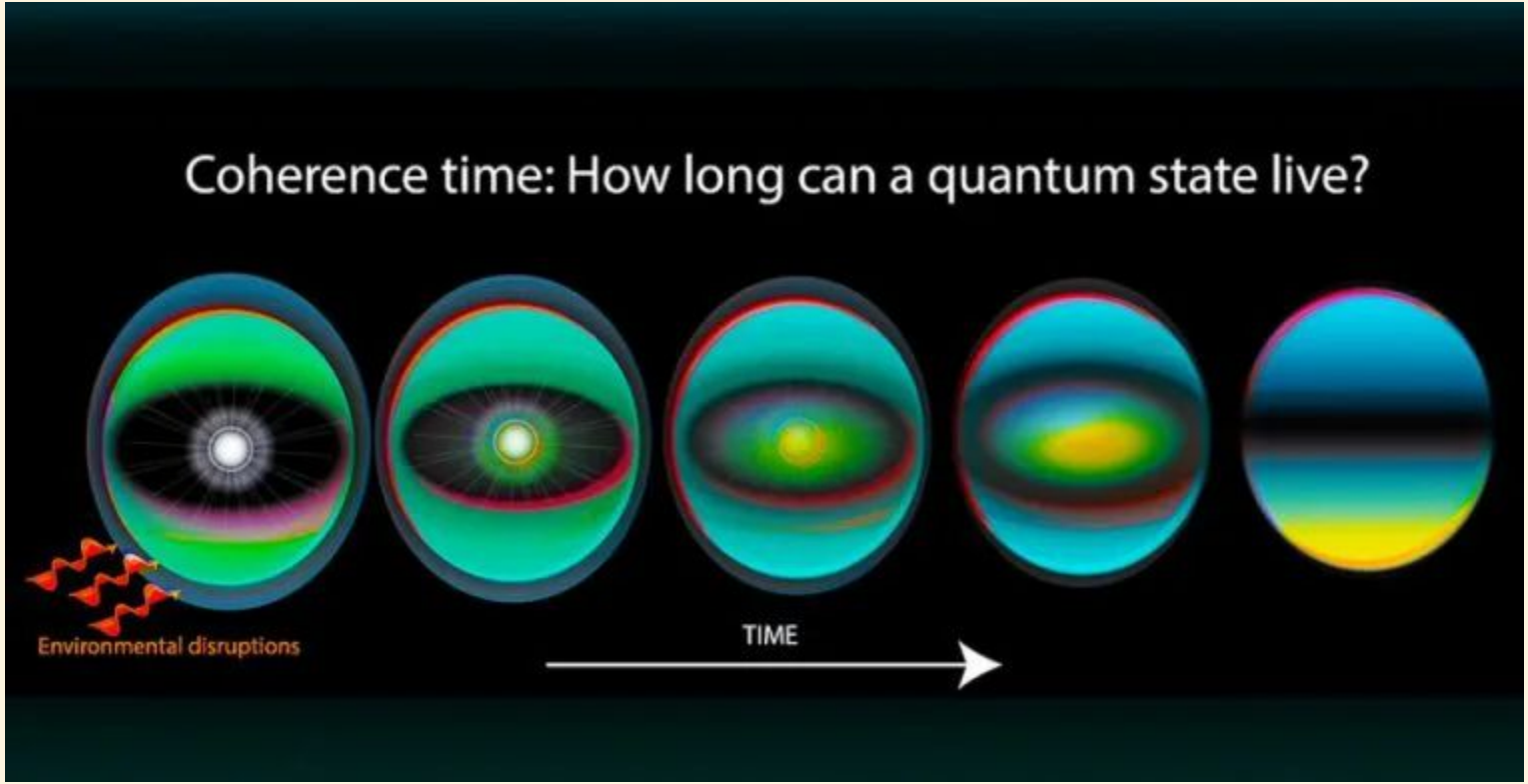
Why don’t we have them today?

Qubit ***relax*** to ground state: |1>→ |0>



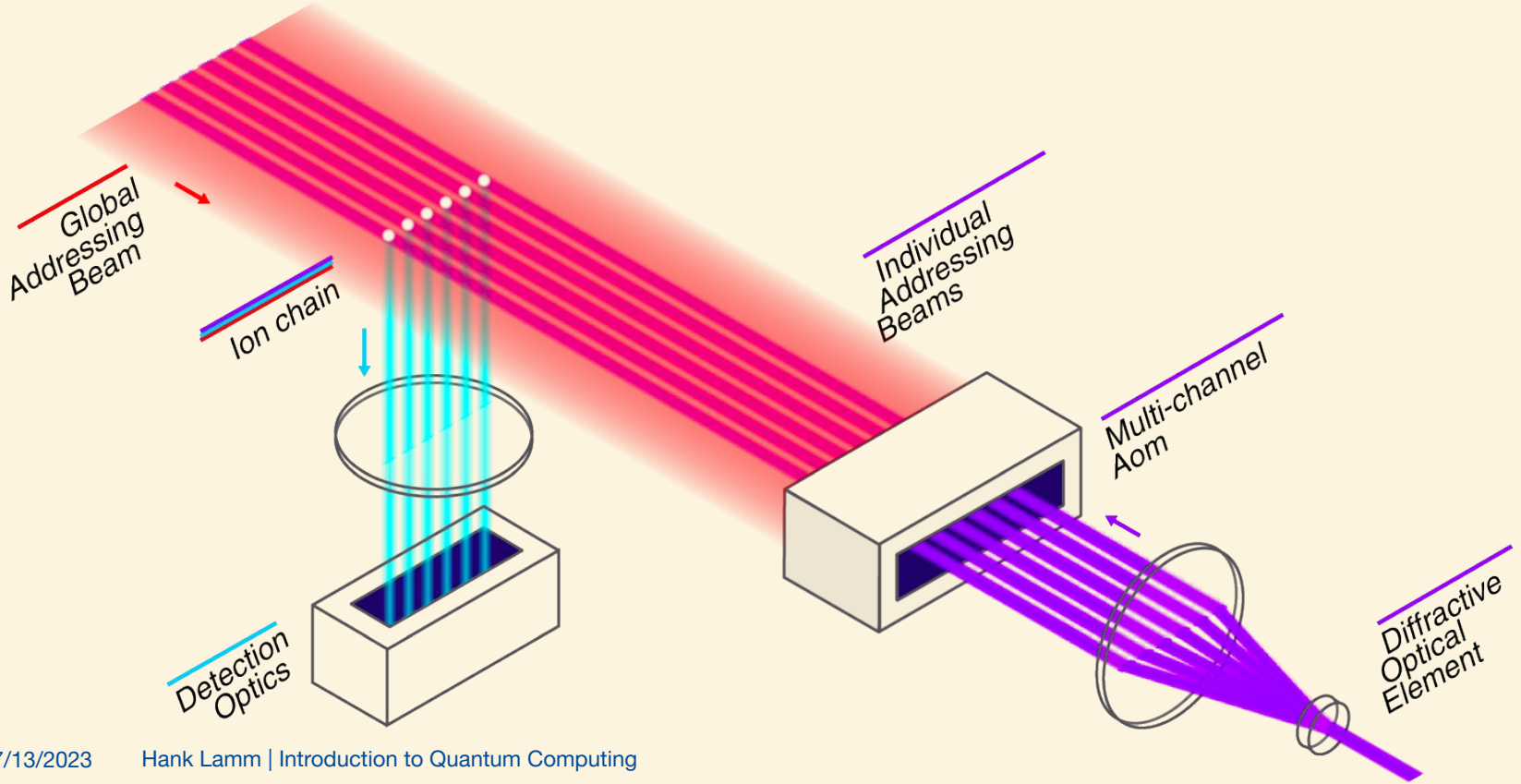
Why don’t we have them today?

Outside world ***heats*** system: |11>+|00>→ |00>



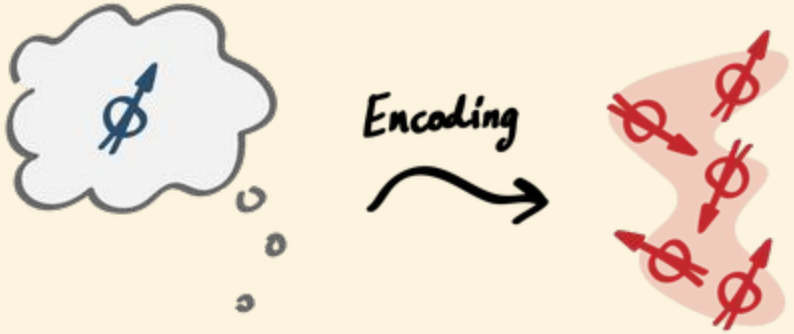
Why don’t we have them today?

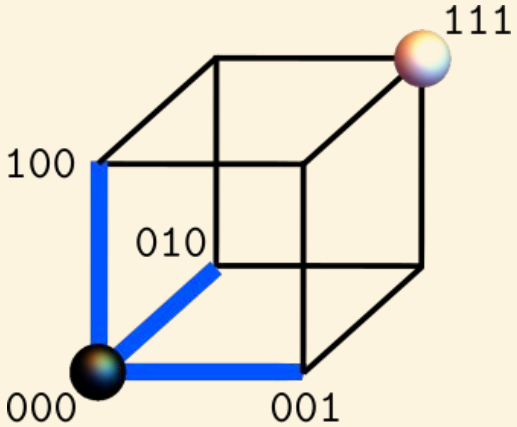
Gates are ***inexact*** instead of U|0>→ |1>, U|0>→ (1-a)|1>+a|0>

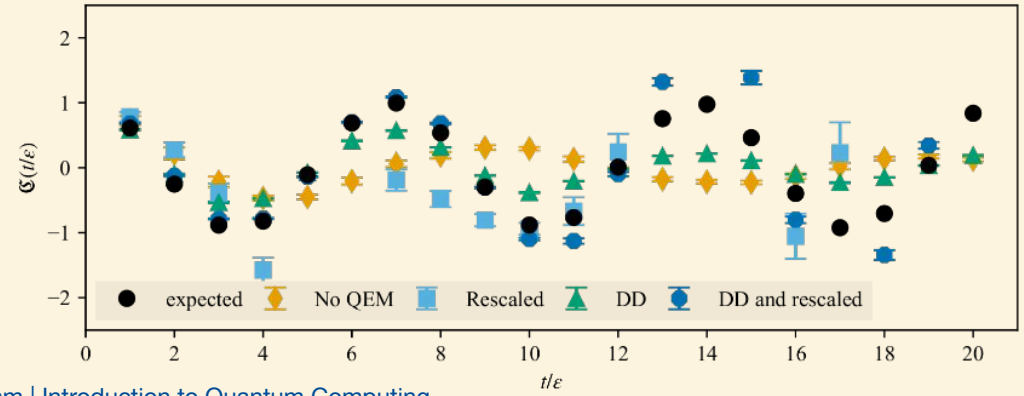


How do I make a better quantum computer?

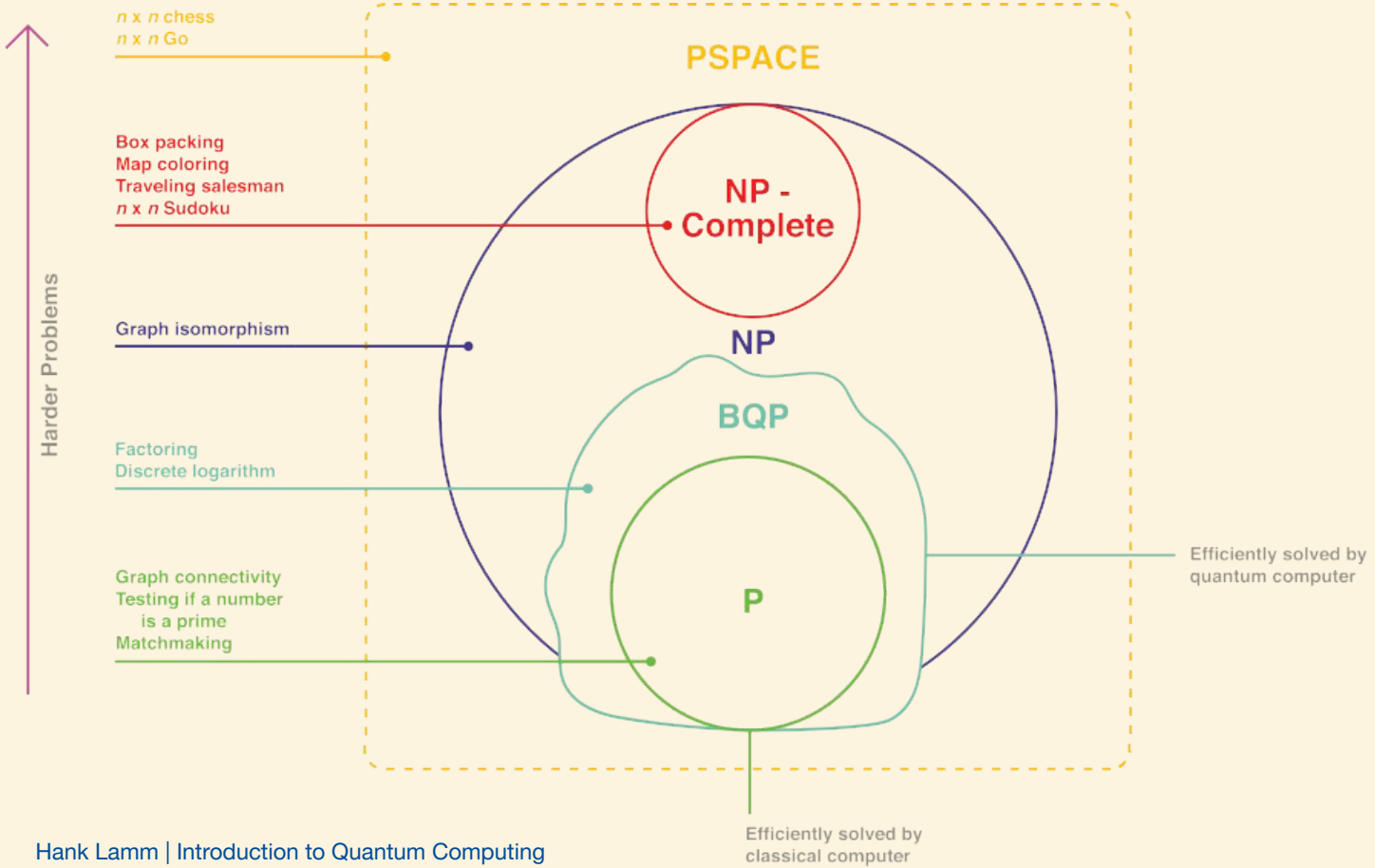
Error correction and mitigation: Finding clever ways to overcome these limitations
This is a hardware/software problem





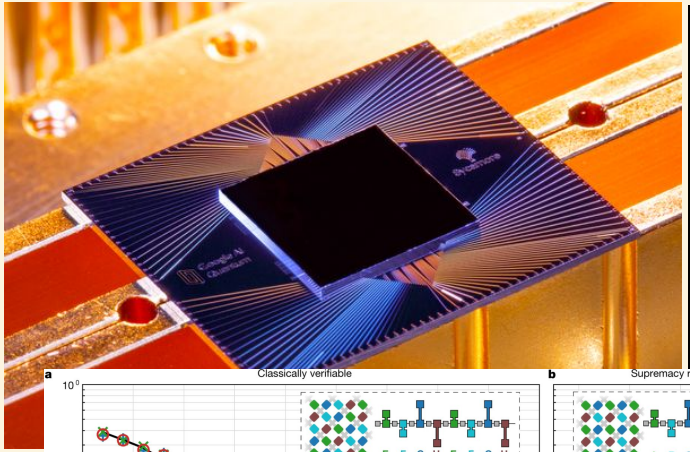


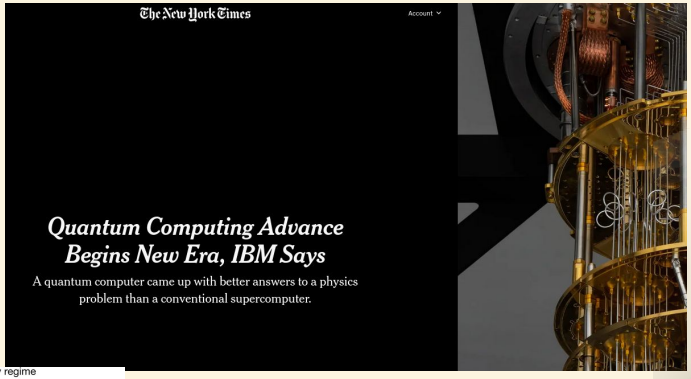
Quantum Complexity

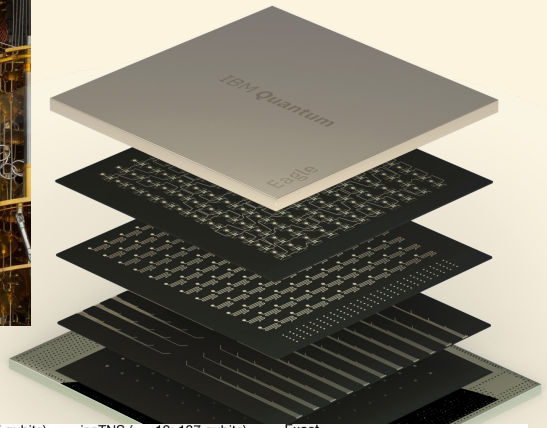


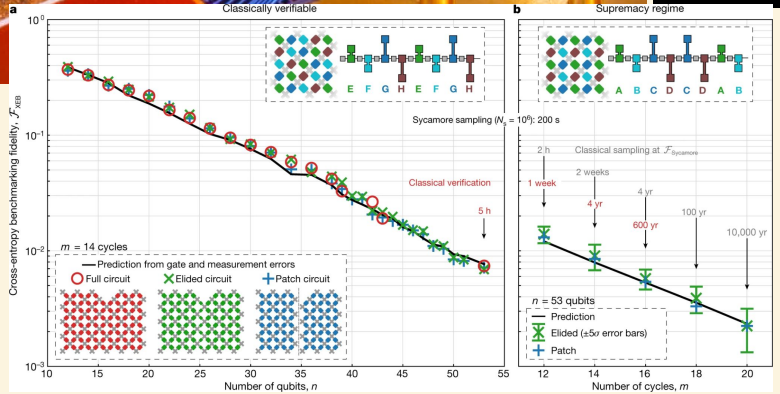
Quantum supremacy, advantage, and practicality

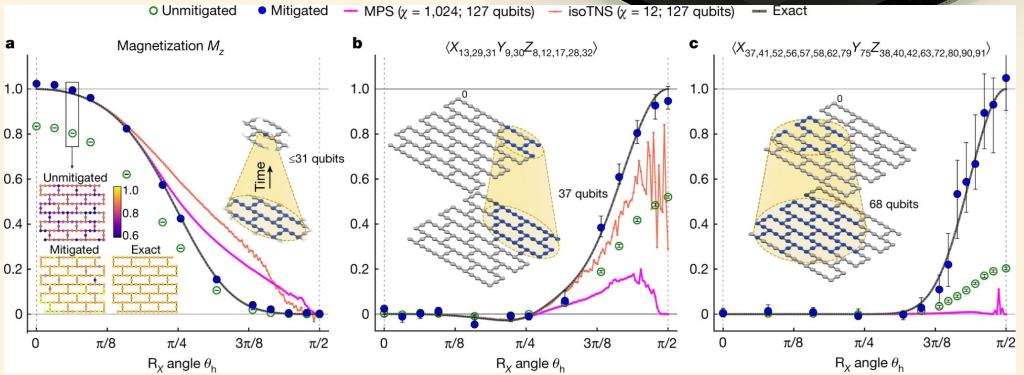
Will happen **soon**, but look out with skepticism





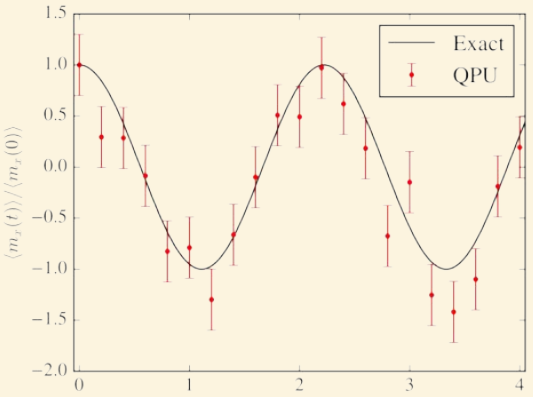




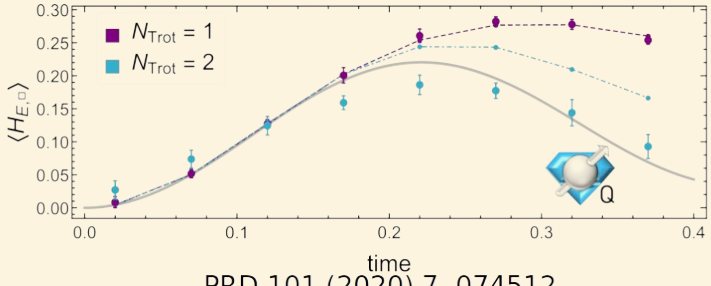


Noisy Intermediate Scale Quantum (NISQ) Era

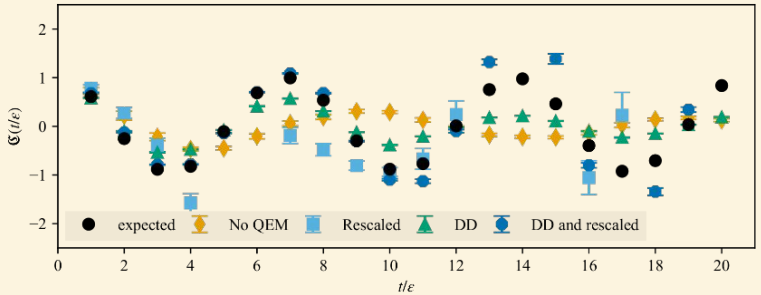
- **NISQ Era:** ~ 1000 qubits, ~1000 gates per qubit
- **Today:** ~100 qubits, ~100 gates per qubit
- **Little/No error correction** thus must mitigate!
- **Quantum Simulators** are critical



PRD 121 (2018) 17, 170501

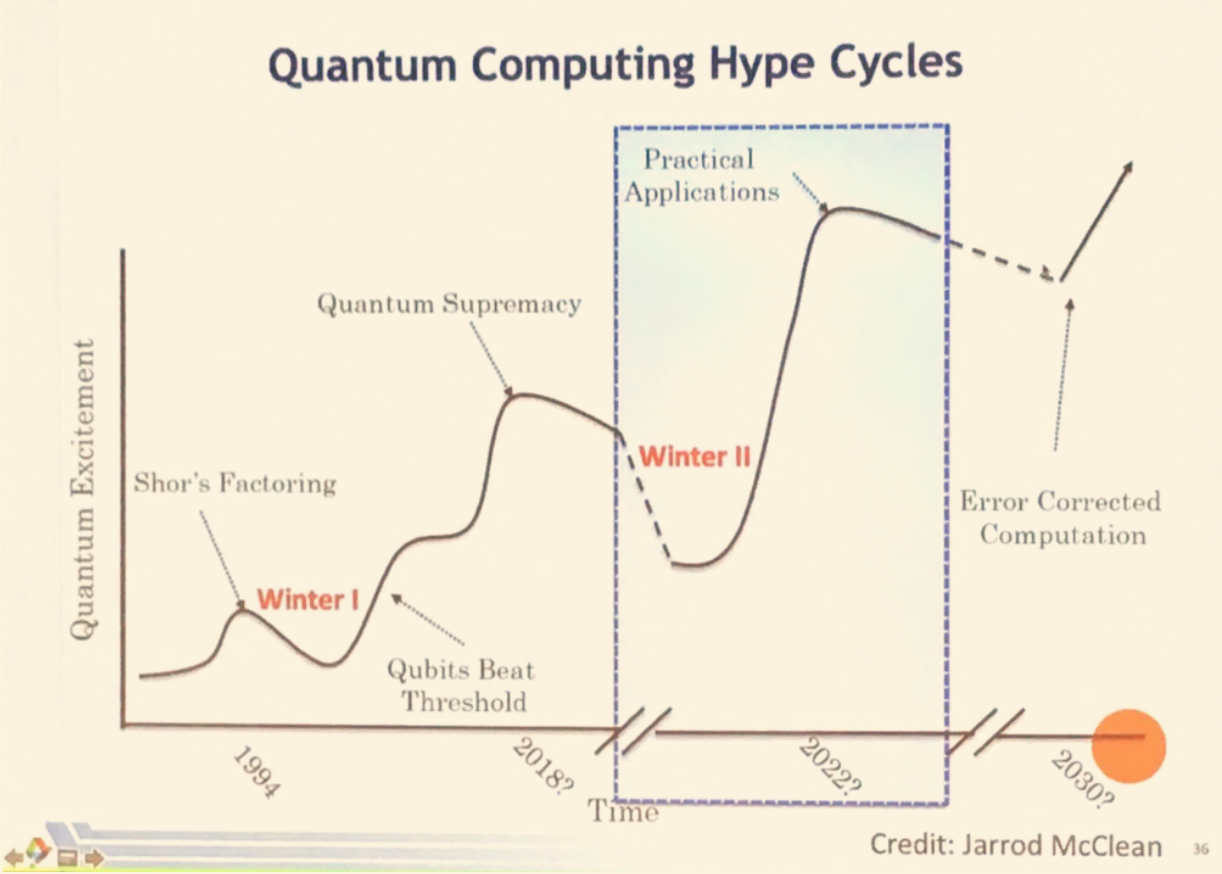


PRD 101 (2020) 7, 074512



2305.02361 [hep-lat]

What is in the future?

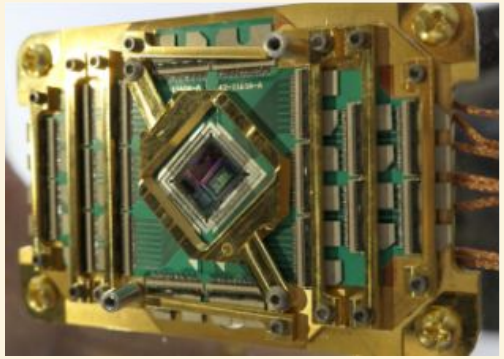


Don’t let anyone fool you…

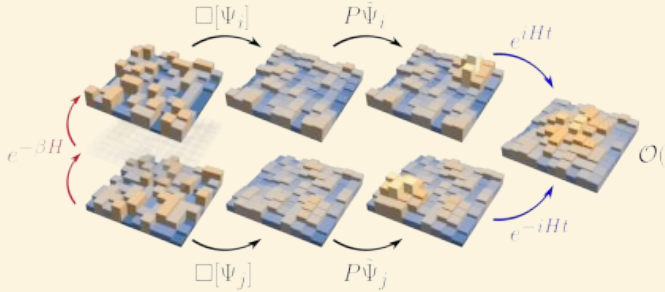
There is **so much** to be done

What can you, yes you, do?

- **Design/experiment** with hardware for better systems
- **Develop** code, compilers, and libraries for a completely new paradigm of computers
- **Invent and analyze** new algorithms for efficiently solve problems today and in the future



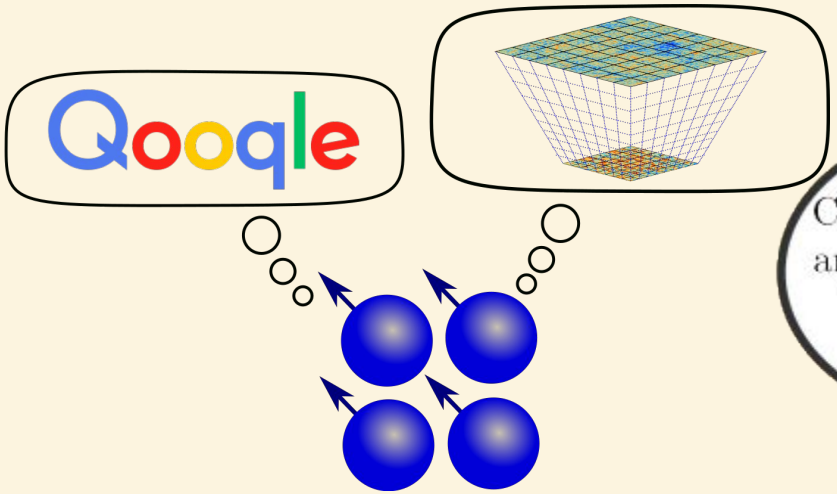
```
from qiskit import QuantumProgram
qp = QuantumProgram()
qr = qp.create_quantum_register('qr', 2)
cr = qp.create_classical_register('cr', 2)
qc = qp.create_circuit('Bell', [qr], [cr])
qc.h(qr[0])
qc.cx(qr[0], qr[1])
qc.measure(qr[0], cr[0])
qc.measure(qr[1], cr[1])
result = qp.execute('Bell')
print(result.get_counts('Bell'))
```

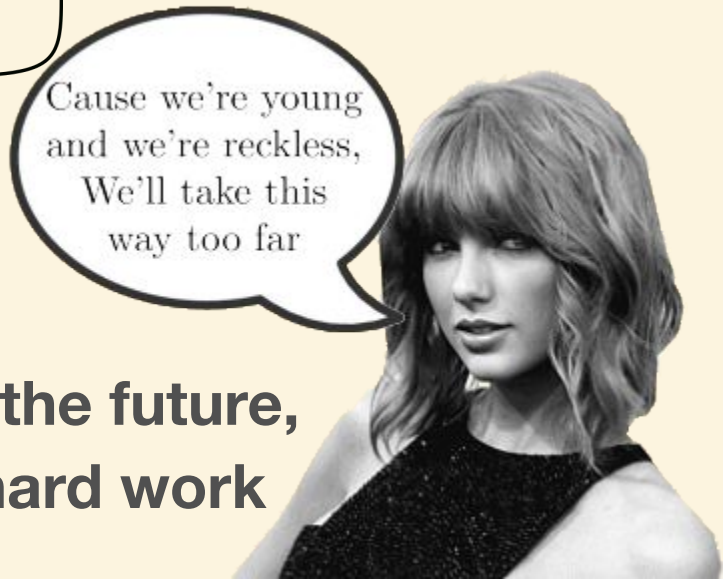


Every one of these topics can use you, right now

We live in exciting times...

- QC is a ***new paradigm*** using quantum mechanics
- May not use them in your day-to-day, but they will revolution the world
- QC is “just starting” and will be active for decades





You should be excited about the future, but it won’t come without hard work