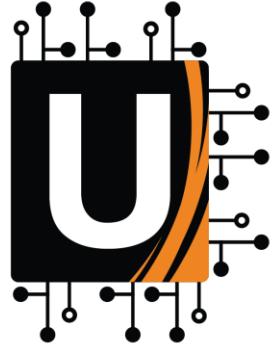


**HighTech**  
Empowering Future Innovators



# What is Quantum Computing?

Priya Angara, Ulrike Stege

# Frequently Asked Questions

---

- Is it real?
- Google just announced Quantum Supremacy. What does that mean?
- Are Qubits in multiple states at once? How can that be possible?
- Is security in our society going to break down?
- How does the cat fit in to quantum computing?



# Quantum Computing in facts and figures



**Between 1,000  
and 100,000**

times more qubits  
needed to correct  
quantum noise  
compared to classic  
computation noise



**-273.15°C**

temperature that  
researchers work  
at to preserve  
quantum state for  
superconducting qubits



**250**

quantum algorithms -  
Quantum computing is not  
universal. It is modified to  
individual algorithms, and  
increases the speed of  
specific calculations.



**1994**

Shor's algorithm -  
factors by prime  
number to crack  
asymmetric  
crypto-systems

# Quantum Physics

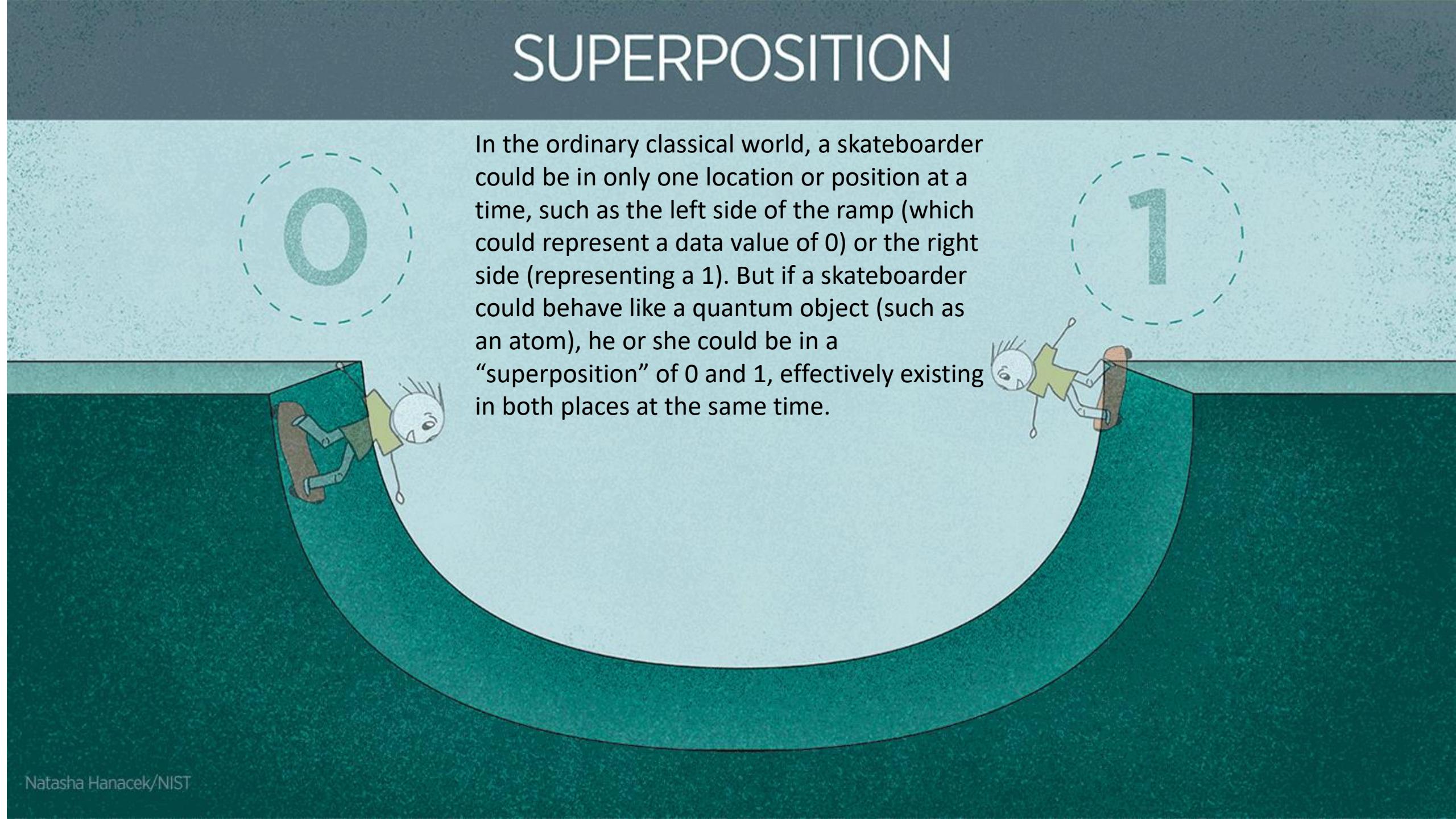


10 influential figures in the history of quantum mechanics.  
Left to right:

Max Planck, Albert Einstein,  
Niels Bohr, Louis de Broglie,  
Max Born, Paul Dirac,  
Werner Heisenberg, Wolfgang Pauli,  
Erwin Schrödinger, Richard Feynman.



# SUPERPOSITION

A cartoon illustration of a skateboarder on a green ramp. The ramp has a dashed circular outline above it. The number '0' is inside the left half of the circle, and the number '1' is inside the right half. The skateboarder is shown in two positions: one where they are leaning towards the left side of the ramp, and another where they are leaning towards the right side. This visualizes how a quantum object like a skateboarder can be in multiple states (0 and 1) simultaneously.

In the ordinary classical world, a skateboarder could be in only one location or position at a time, such as the left side of the ramp (which could represent a data value of 0) or the right side (representing a 1). But if a skateboarder could behave like a quantum object (such as an atom), he or she could be in a “superposition” of 0 and 1, effectively existing in both places at the same time.

# ENTANGLEMENT



# Computer Science

Charles Babbage invents the Analytical Engine

1837

Ada Lovelace develops the first computer algorithm

1843

1936

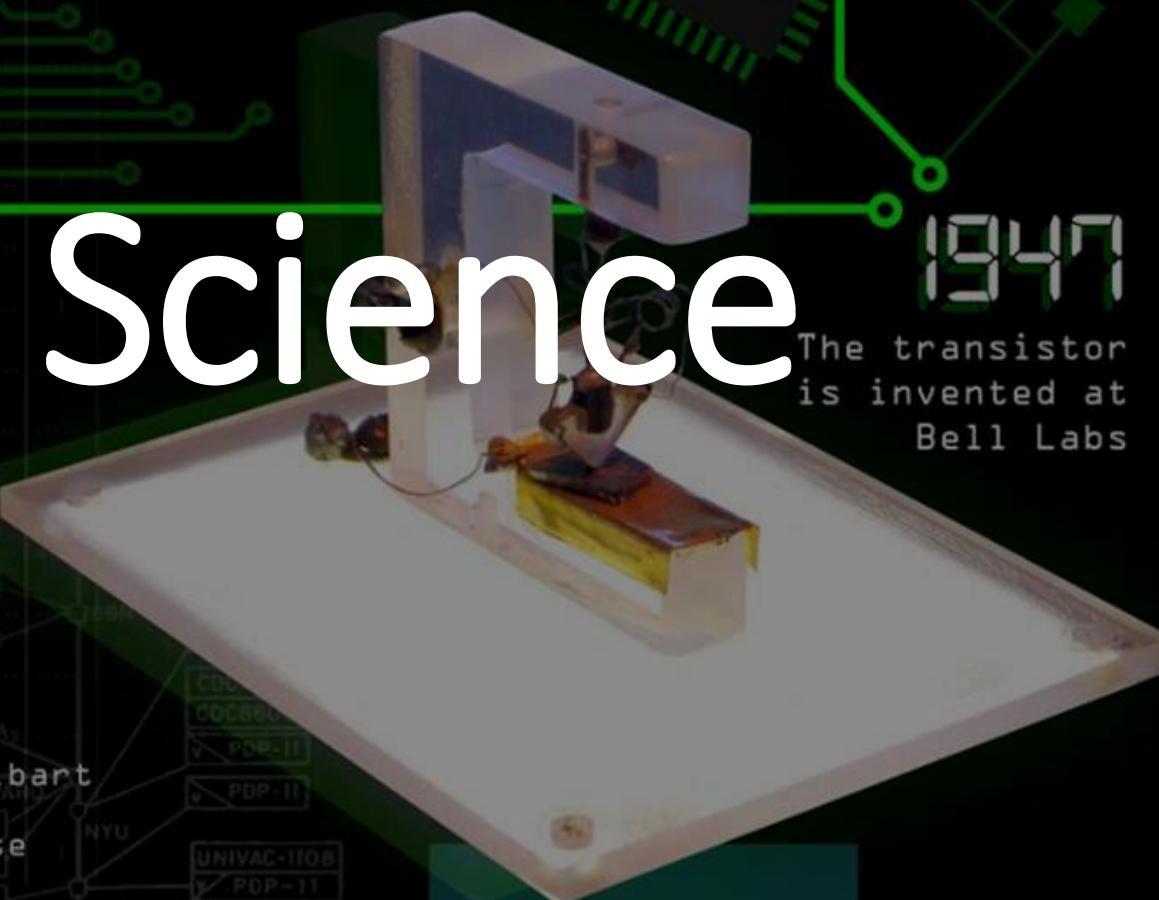
Alan Turing invents the Turing Machine

1947

The transistor is invented at Bell Labs

Steve Wozniak designed the Apple-1, a single-board computer for hobbyists

1837



Douglas Engelbart invents the computer mouse

1968

DARPA creates ARPAnet, the first operational computer network and ancestor

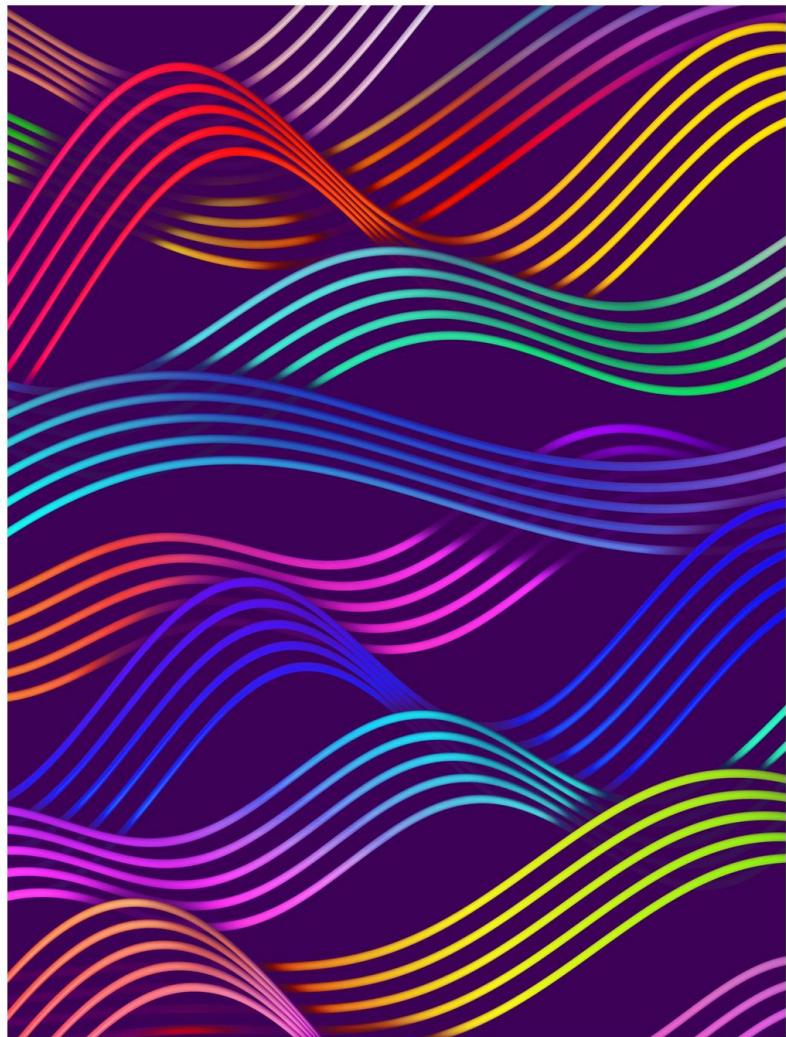
N

Marc Andresson created Mosaic, later known as

# Computer Science

---

128    64    32    16    8    4    2    1



# MuseNet

We've created MuseNet, a deep neural network that can generate 4-minute musical compositions with 10 different instruments, and can combine styles from country to Mozart to the Beatles. MuseNet was not explicitly programmed with our understanding of music, but instead discovered patterns of harmony, rhythm, and style by learning to predict the next token in hundreds of thousands of MIDI files. MuseNet uses the same general-purpose unsupervised technology as GPT-2, a large-scale transformer model trained to predict the next token in a sequence, whether audio or text.

APRIL 25, 2019

6 MINUTE READ, 16 MINUTE LISTEN

# Prime Factorization

## Insert Web Page

This app allows you to insert secure web pages starting with https:// into the slide deck. Non-secure web pages are not supported for security reasons.

Please enter the URL below.

bit.ly/2OB3nOi

Note: Many popular websites allow secure access. Please click on the preview button to ensure the web page is accessible.

COMPUTER  
SCIENCE

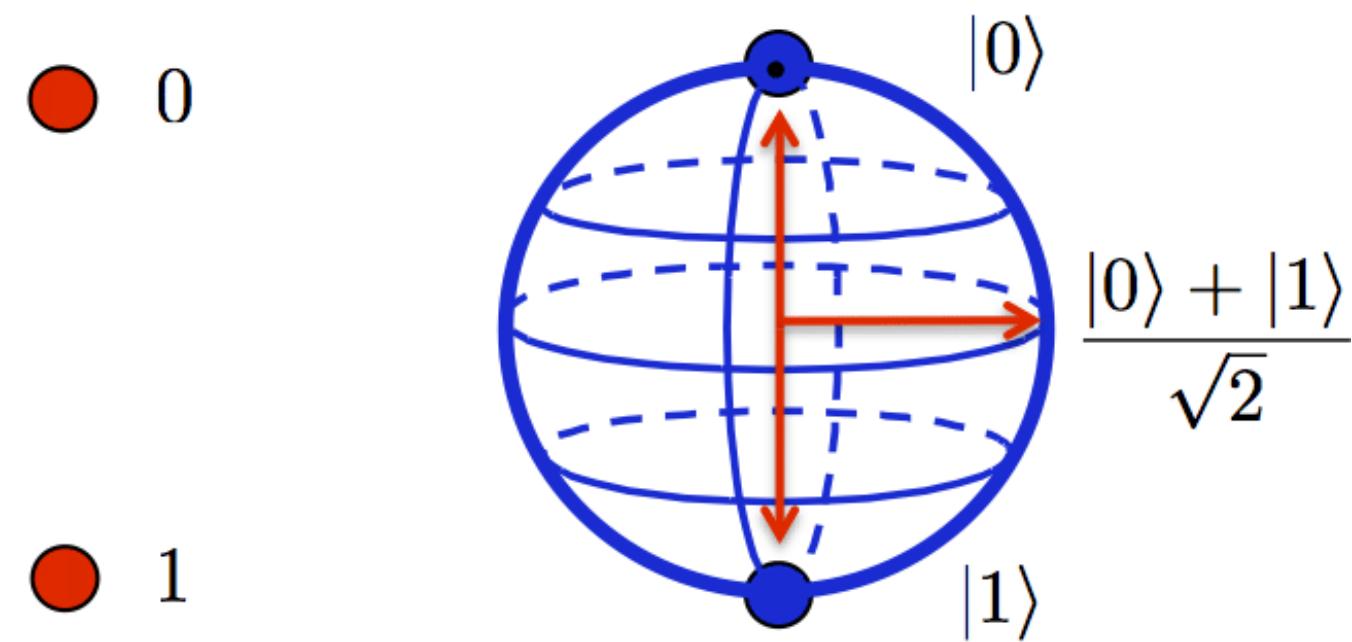
QUANTUM  
PHYSICS

# Quantum Computing!



IBM Quantum Computing Scientists Hanhee Paik (left) and Sarah Sheldon (right) examine the hardware inside an open dilution fridge at the IBM Q Lab at IBM's T. J. Watson Research Center in Yorktown, NY.

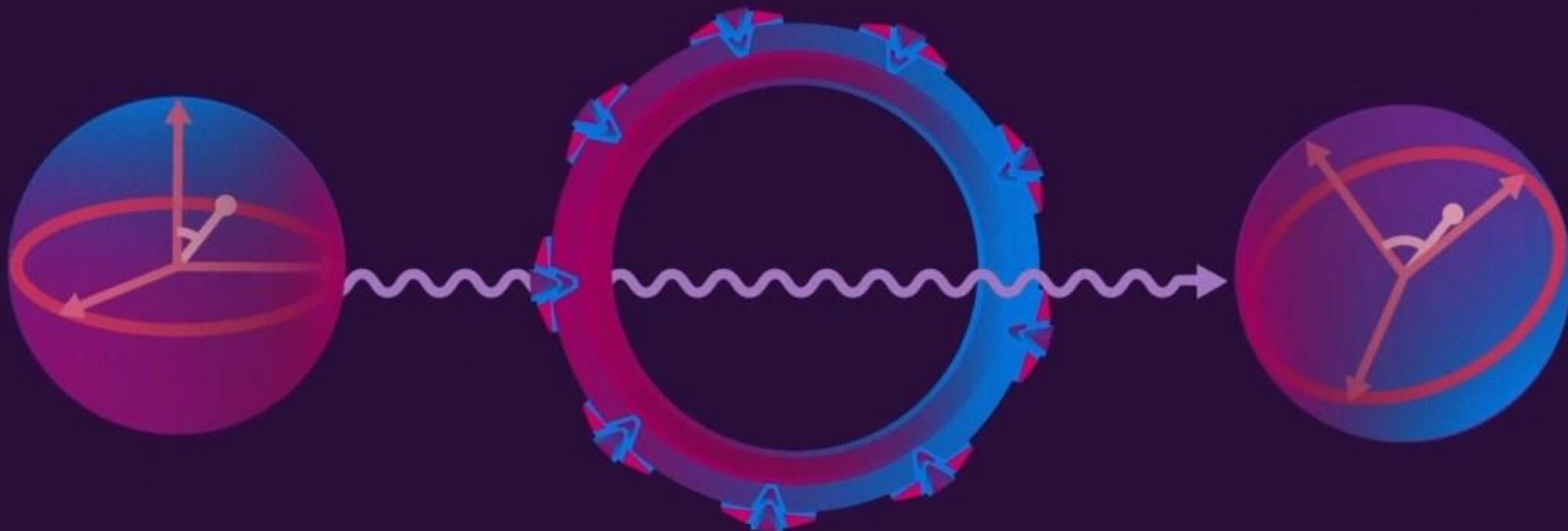
# Qubits



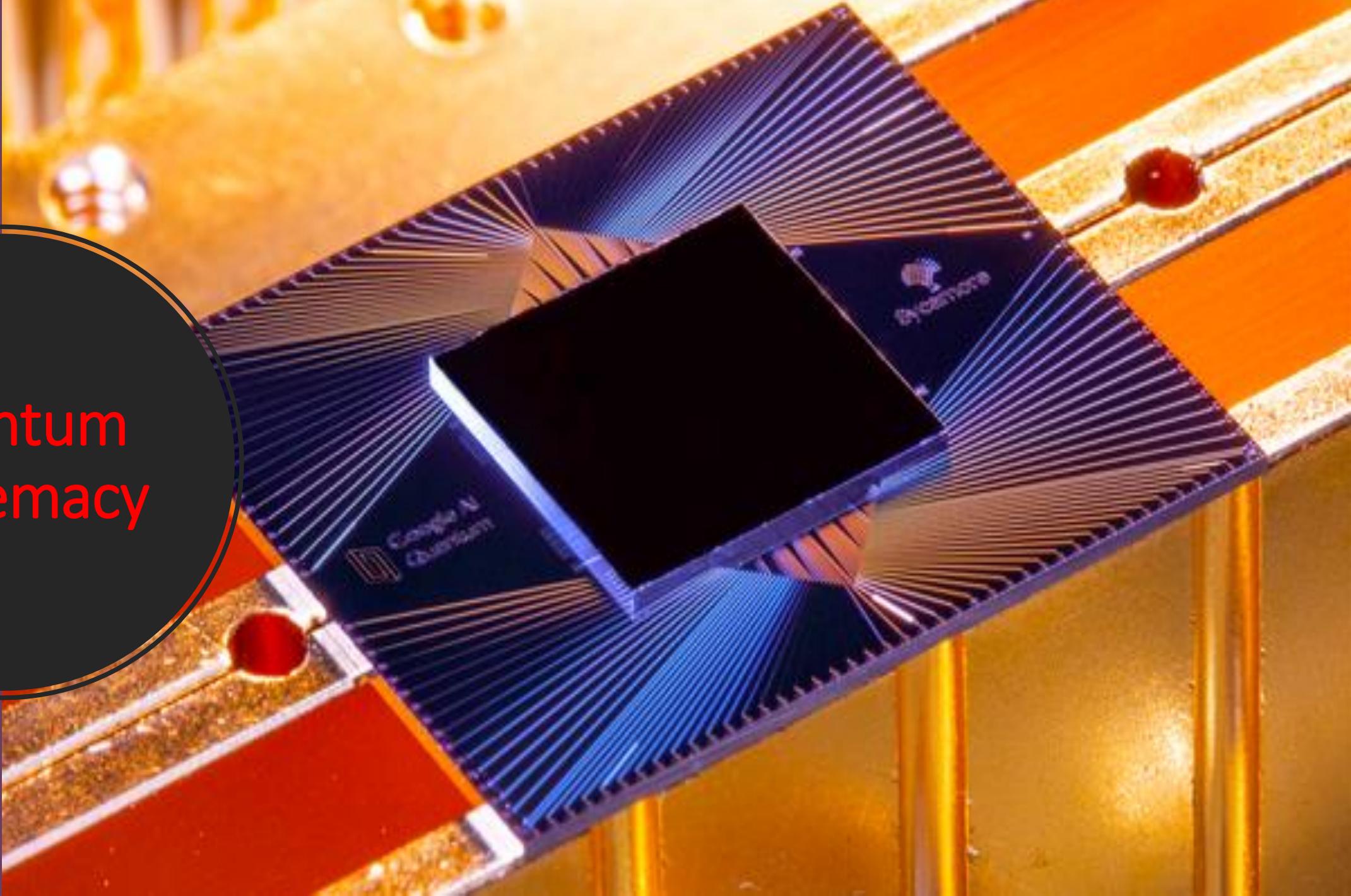
**Classical Bit**

**Qubit**

# QUANTUM GATE



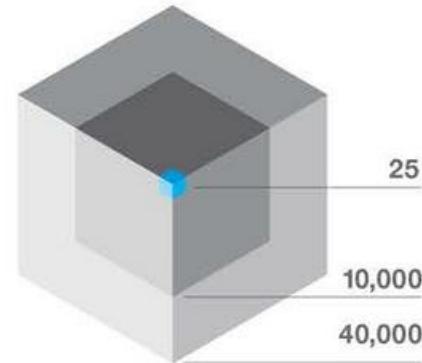
# Quantum Supremacy



# A Quantum Computer's power depends on more than just adding qubits

If we want to use quantum computers to solve real problems, they will need to explore a large space of quantum states. The number of qubits is important, but so is the error rate. In practical devices, the effective error rate depends on the accuracy of each operation, but also on how many operations it takes to solve a particular problem as well as how the processor performs these operations. Here we introduce a quantity called **Quantum Volume** which accounts for all of these things. Think of it as a representation of the problem space these machines can explore.

**Quantum Volume**  
Volume of cube proportional to useful quantum computing that can be done



Quantum Volume  
by error rate (y axis)  
and qubit count (x axis)

LOW

HIGH

Source:  
IBM Research

0.00001

0.0001

0.001

0.01

0.1

QUBITS

5

15

25

50

100

200

500

Improving the error rate will result in a more powerful Quantum Computer

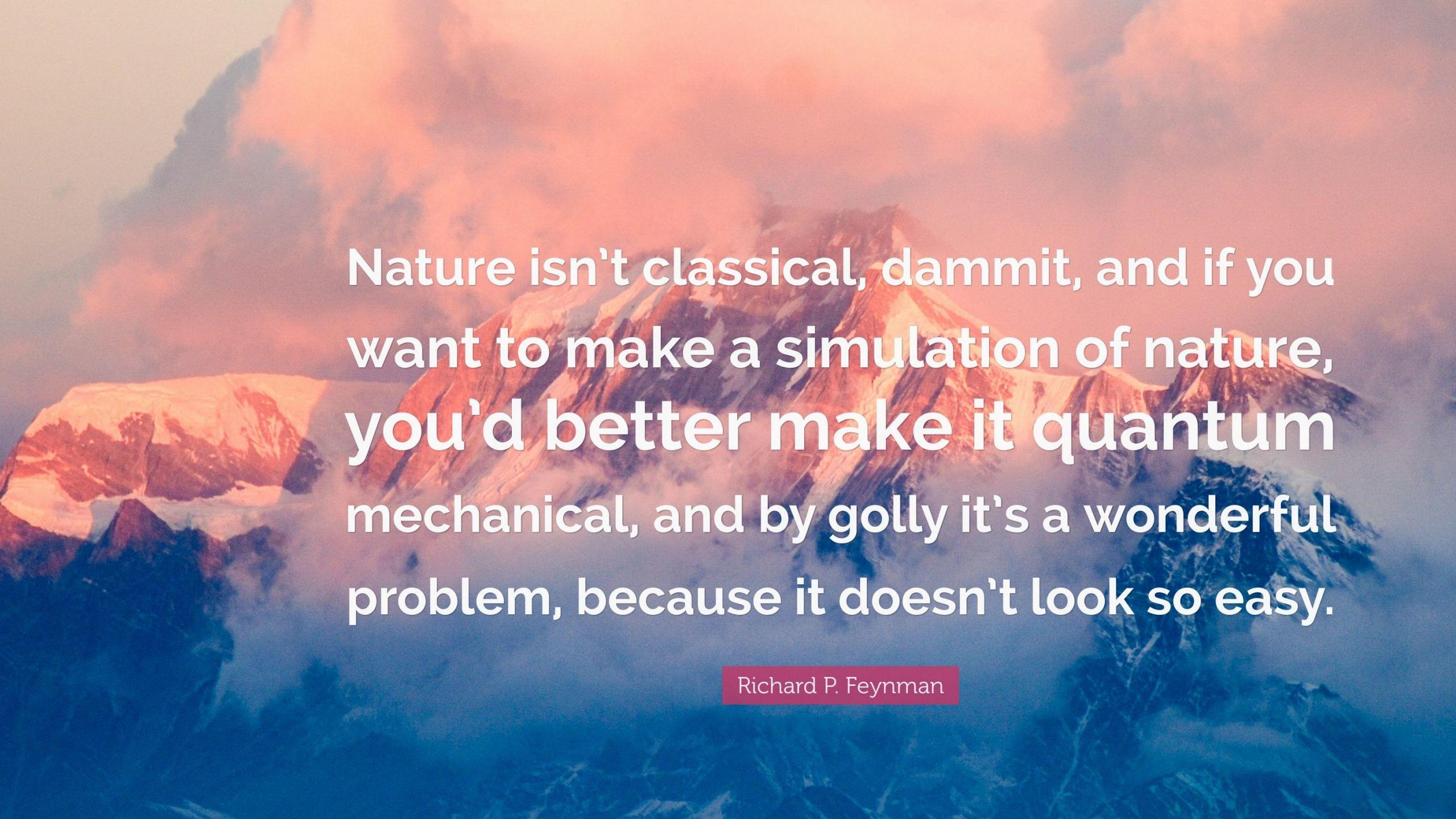
Qubits Added: 0  
Error Rate Decrease: 10x  
Quantum Volume Increase: 24x

Increasing qubit number does not improve a Quantum Computer if error rate is high

Qubits Added: 100  
Error Rate Decrease: 0  
Quantum Volume Increase: 0

# Applications





**Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.**

Richard P. Feynman

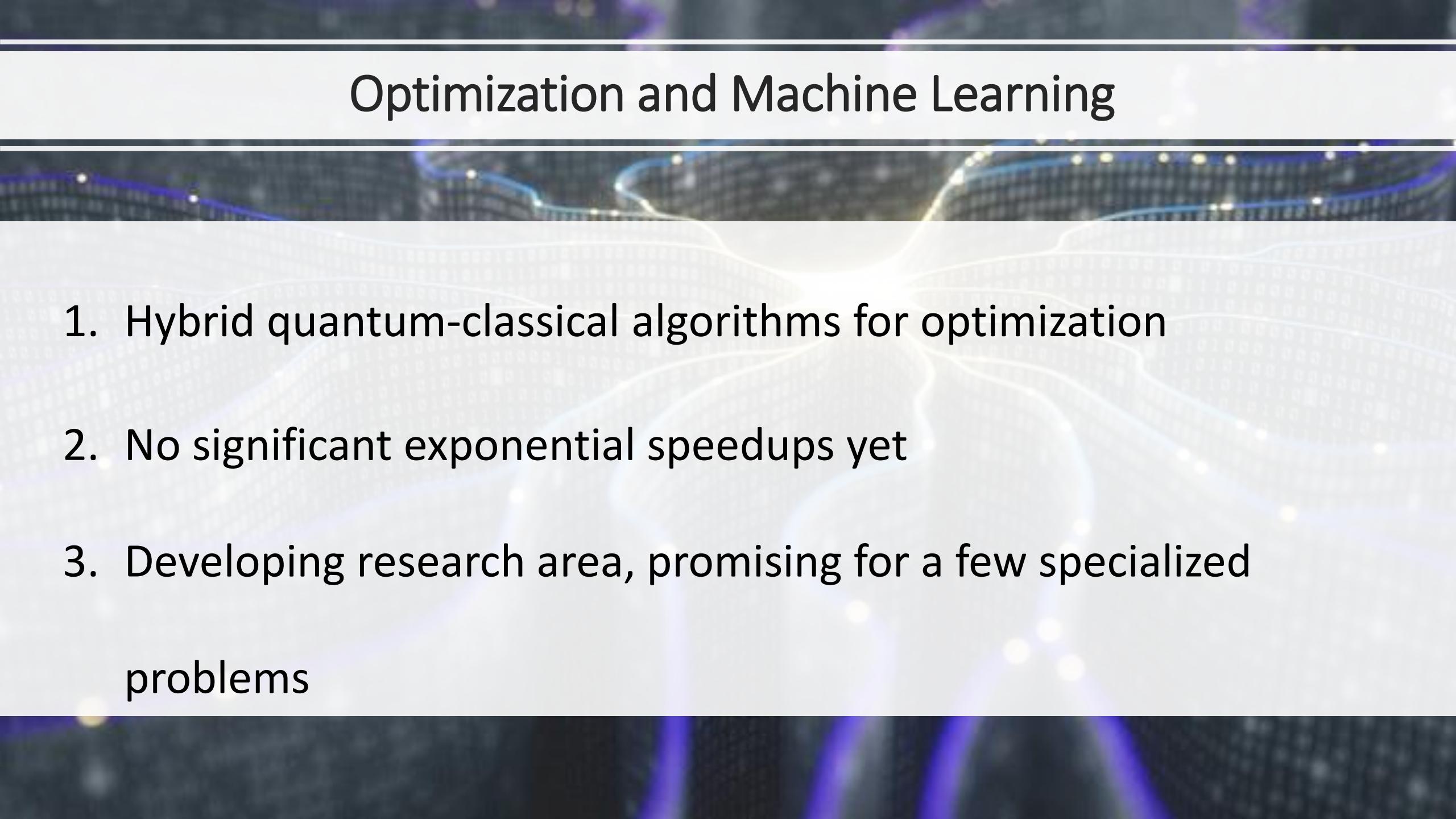
# Simulating Quantum Phenomena

1. Direct mapping between molecular wave functions and qubits
2. Number of gates scales polynomially with system size
3. Quantum Chemistry applications: simulating molecules

# (Post) Quantum Cryptography

1. Perfect quantum computers will break current classical cryptography techniques
2. Research avenues:
  1. PQC: Modify existing protocols so that quantum computers cannot break them
  2. QC: Setup new communications infrastructure which promises security based on quantum physics

# Optimization and Machine Learning



1. Hybrid quantum-classical algorithms for optimization
2. No significant exponential speedups yet
3. Developing research area, promising for a few specialized problems

# IBM Q Experience

IBM Q Experience    5\_pulse\_sche...    declarative\_a...    programmatic...    max\_cut\_and...    1\_start\_here.i...    \* HightechU    Open

New    Save    Clear    Delete    Help

HightechU    Unsaved changes Run →

Circuit editor    X    Circuit composer    Gates overview

```
OPENQASM 2.0;
include "qelib1.inc";
gate nG0(param) q {
    h q;
}

qreg q[5];
creg c[5];

h q[1];
cx q[2],q[3];
id q[1];
t q[1];
ch q[0],q[1];
u1(pi/2) q[1];
```

Gates

H	S	S <sup>†</sup>				X	Y	Z	ID	U1	U2	U3
Rx	Ry	Rz		T	T <sup>†</sup>	cH	cRz					

Barrier    Operations    Subroutines

|    | $\otimes$     if     $\text{not}^z$     nG0    + Add

q[0] |0>  
q[1] |0>  
q[2] |0>  
q[3] |0>  
q[4] |0>

Quantum computing devices

<https://quantum-computing.ibm.com/>

Circuit Composer

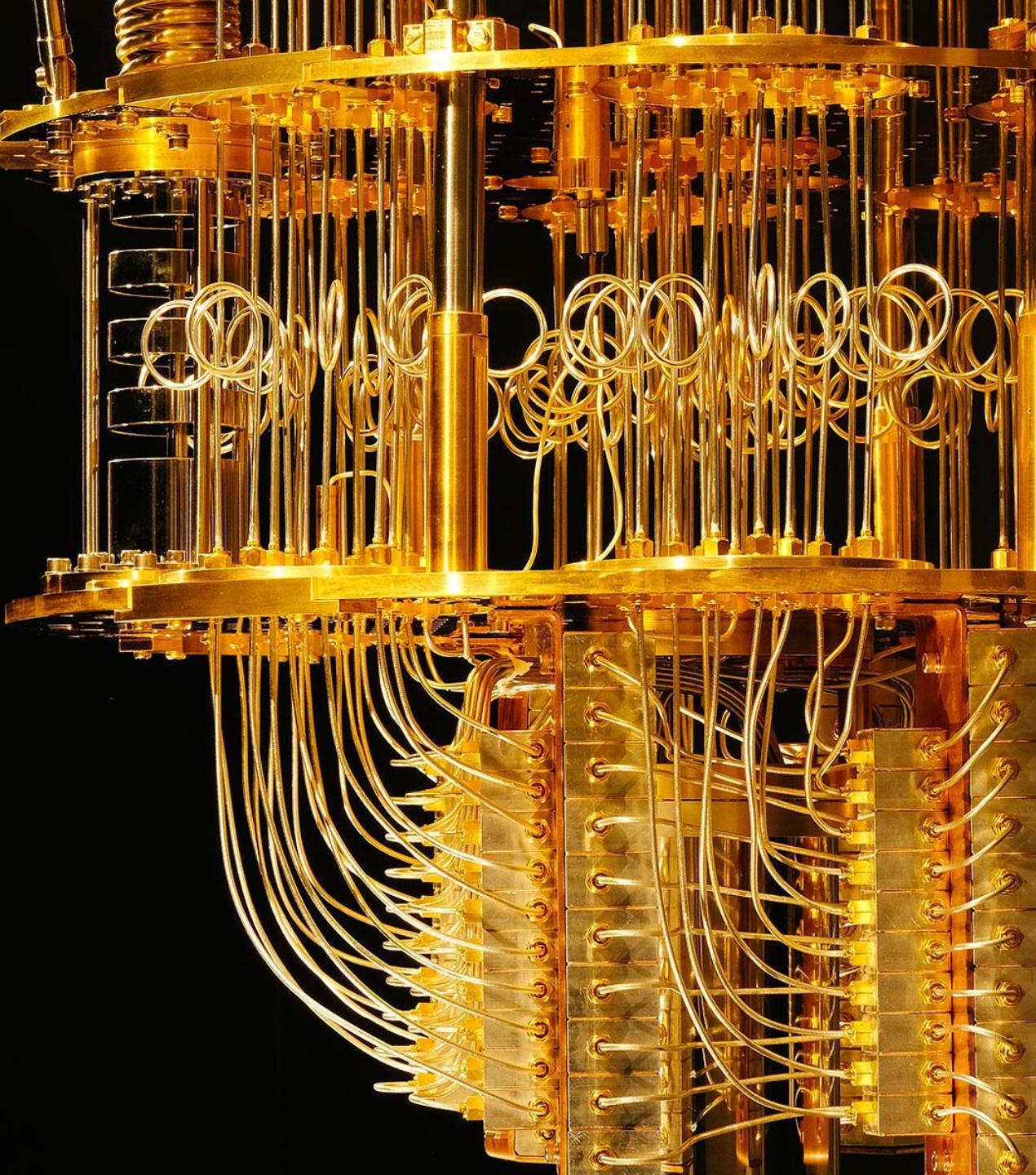
<https://quantum-computing.ibm.com/composer>

Qiskit

<https://qiskit.org/>

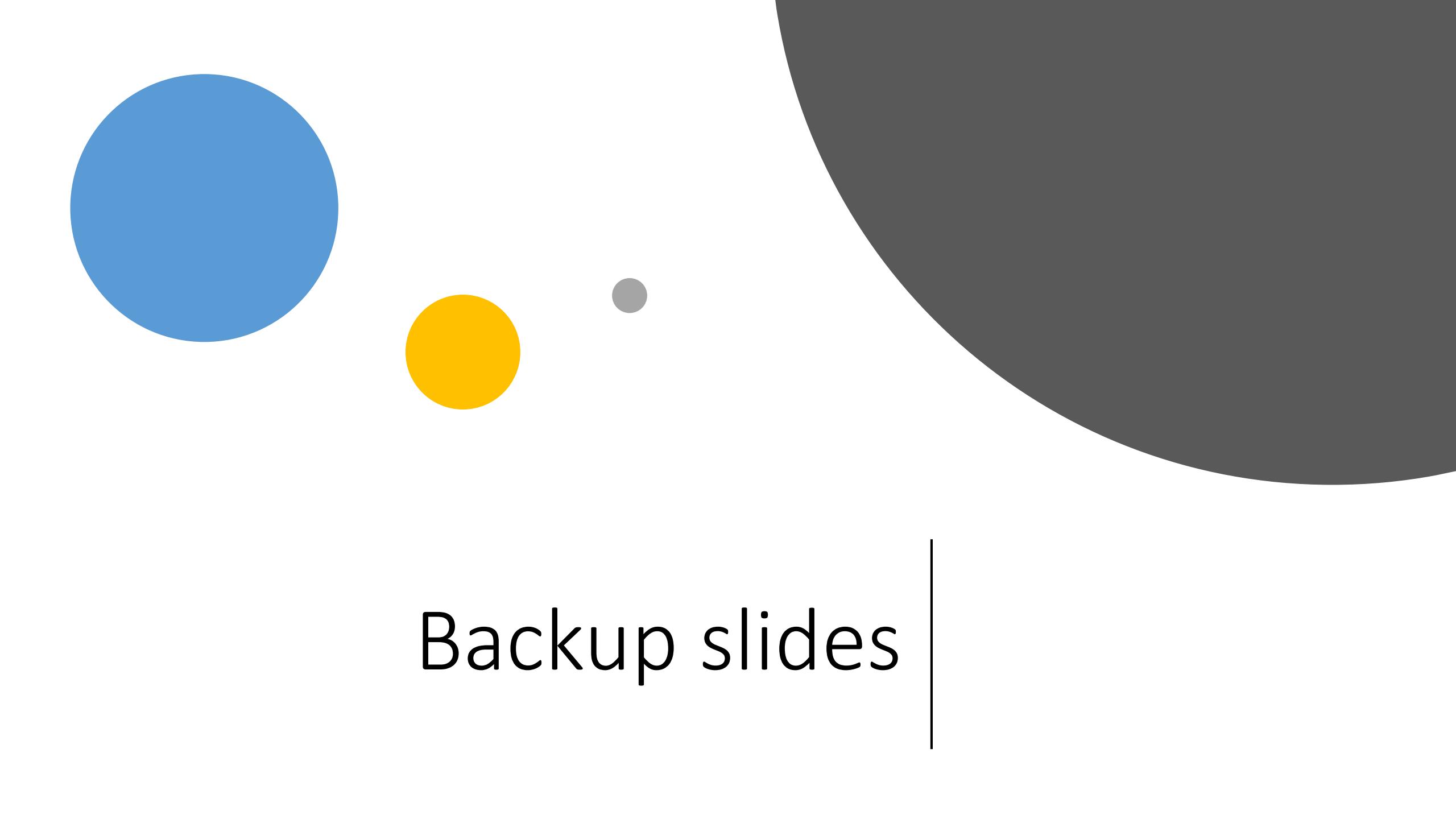
Shtetl-Optimized

<https://www.scottaaronson.com/blog/>





Thank You



The background features a large blue circle on the left, a smaller yellow circle below it, a tiny gray dot between them, and a large dark gray shape on the right.

Backup slides

# Timeline

	<b>1900</b>	Planck proposes that radiation comes in discrete amounts, or is quantized
	<b>1924</b>	Louis de Broglie proposes that matter has wave properties
	<b>1960</b>	First laser built
	<b>1981</b>	Richard Feynman invents the concept of a quantum computer
	<b>1994</b>	Peter Shor invents the first “useful” quantum algorithm to crack prime number-based cryptographies
	<b>1905</b>	Einstein suggests a quantum of light (the photon)
	<b>1926</b>	Erwin Schrödinger develops wave mechanics
	<b>1973</b>	GPS launched by US Department of Defense
	<b>1981</b>	Alain Aspect demonstrates the existence of the entanglement phenomenon
	<b>2001</b>	First execution of Shor algorithm on a quantum device, Stanford University

# The three known types of quantum computing and their applications, generality, and computational power.



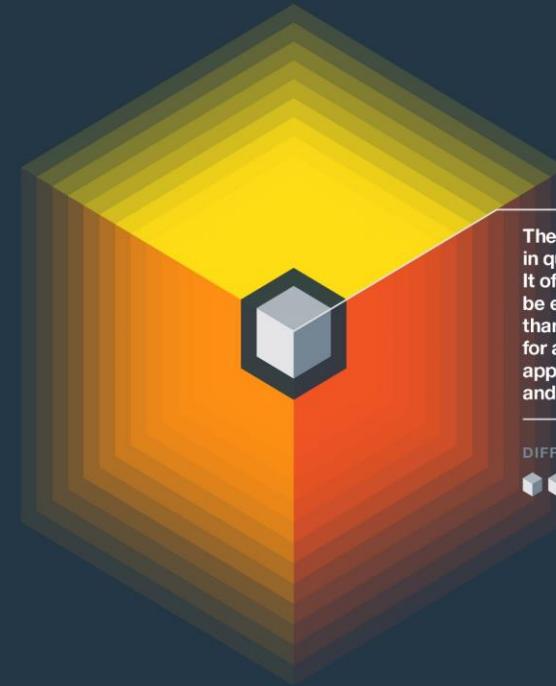
A very specialized form of quantum computing with unproven advantages over other specialized forms of conventional computing.

#### DIFFICULTY LEVEL



The most likely form of quantum computing that will first show true quantum speedup over conventional computing. This could happen within the next five years.

#### DIFFICULTY LEVEL



The true grand challenge in quantum computing. It offers the potential to be exponentially faster than traditional computers for a number of important applications for science and businesses.

#### DIFFICULTY LEVEL



## Quantum Annealer

The quantum annealer is least powerful and most restrictive form of quantum computers. It is the easiest to build, yet can only perform one specific function. The consensus of the scientific community is that a quantum annealer has no known advantages over conventional computing.

#### APPLICATION

Optimization Problems

#### GENERALITY

Restrictive

#### COMPUTATIONAL POWER

Same as traditional computers

## Analog Quantum

The analog quantum computer will be able to simulate complex quantum interactions that are intractable for any known conventional machine, or combinations of these machines. It is conjectured that the analog quantum computer will contain somewhere between 50 to 100 qubits.

#### APPLICATIONS

Quantum Chemistry  
Material Science  
Optimization Problems  
Sampling  
Quantum Dynamics

#### GENERALITY

Partial

#### COMPUTATIONAL POWER

High

## Universal Quantum

The universal quantum computer is the most powerful, the most general, and the hardest to build, posing a number of difficult technical challenges. Current estimates indicate that this machine will comprise more than 100,000 physical qubits.

#### APPLICATIONS

Secure computing  
Machine Learning  
Cryptography  
Quantum Chemistry  
Material Science  
Optimization Problems  
Sampling  
Quantum Dynamics  
Searching

#### GENERALITY

Complete with known speed up

#### COMPUTATIONAL POWER

Very High