

HOW DID QUANTUM COMPUTING COME TO BE?



From atoms to algorithms:

A brief history of quantum computing

IN THE EARLY 1900s, THE WORLD OF PHYSICS WAS TURNED...



SCIENTISTS FOUND OUT THAT AS THINGS GET SMALLER AND SMALLER CLASSICAL PHYSICS DOES NOT HOLD!

Energy is quantized!!

Until measured an electron can be in many places at the same time!

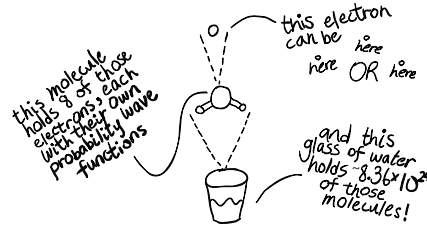
You can never know both the position and momentum of a particle with certainty!

PLANCK

HEISENBERG

SCHRODINGER

THE IDEA THAT SO MANY THINGS WERE PROBABLE AND UNCERTAIN WAS BIZARRE ...



BUT EVEN WITH GREATLY RENOWNED SKEPTICS,

God does not play dice with the universe!

Einstein, stop telling God what to do with his dice!

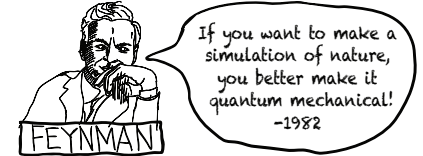
QUANTUM MECHANICS WAS BORN.

EINSTEIN

BOHR

WHILE COMPUTERS ADVANCED, SIMULATING EVEN SIMPLE MOLECULAR SYSTEMS WITH SO MANY PROBABILITIES WAS NEARLY IMPOSSIBLE!

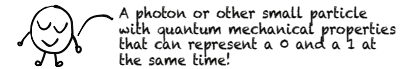
THEN, RICHARD FEYNMAN PROPOSED AN INTERESTING IDEA



INSTEAD OF BITS SET TO 0'S OR 1'S LIKE NORMAL COMPUTERS,



A QUANTUM BIT (QUBIT) WOULD MAKE UP A QUANTUM COMPUTER



AND SO COMPUTERS WOULD MIMIC NATURE'S PROBABILITIES ...

DAVID DEUTSCH LAID OUT A BASIC THEORETICAL STRUCTURE OF A QUANTUM COMPUTER (1985)

And I developed one of the first quantum algorithms with Josza!

DEUTSCH

D-J ALGORITHM

I'm exponentially faster than any deterministic classical algorithm!

THIS IS QUANTUM SUPREMACY

I can do things in a week that classical computers need hundreds of years to do!

THEN IN 1994 ...

SHOR

wait... is that a key?!!

11300477
18807

11453300939

I developed a quantum algorithm to factor multiples of large prime numbers!!

AND THE WORLD WENT BERSERK BECAUSE RSA ENCRYPTION SCHEMES WERE BUILT ON THE ASSUMPTION THAT CLASSICAL COMPUTERS WOULD TAKE AGES TO FACTOR SUCH NUMBERS!

Ahhhhh!

Quick! More quantum computing!

THE ACTUAL HARDWARE IS NOT YET CAPABLE OF SUCH BIG CALCULATIONS ...

Hey, we got a 50-qubit computer!

2017

2018

I think we got a 72-qubit processor!

But is it stable? Universal? How many gates?

Oh wow, we need many thousands of qubits to perform shor's algorithm!

And we need stable machines!

BUT WITH RAPID ADVANCES, QUANTUM COMPUTING IS CONSTANTLY SHOWING NEW POSSIBILITIES ...

AND THE QUANTUM COMPUTING RACE HAS ONLY JUST BEGUN

<https://www.epiqc.cs.uchicago.edu/resources/>

November 2020 (v3)

This work is funded in part by EPIQC, an NSF Expedition in Computing, under grant 1730449

