4COSC003W TRENDS IN COMPUTER SCIENCE: QUANTUM COMPUTING

DR PHILIP TRWOGA

DEPARTMENT OF COMPUTER SCIENCE

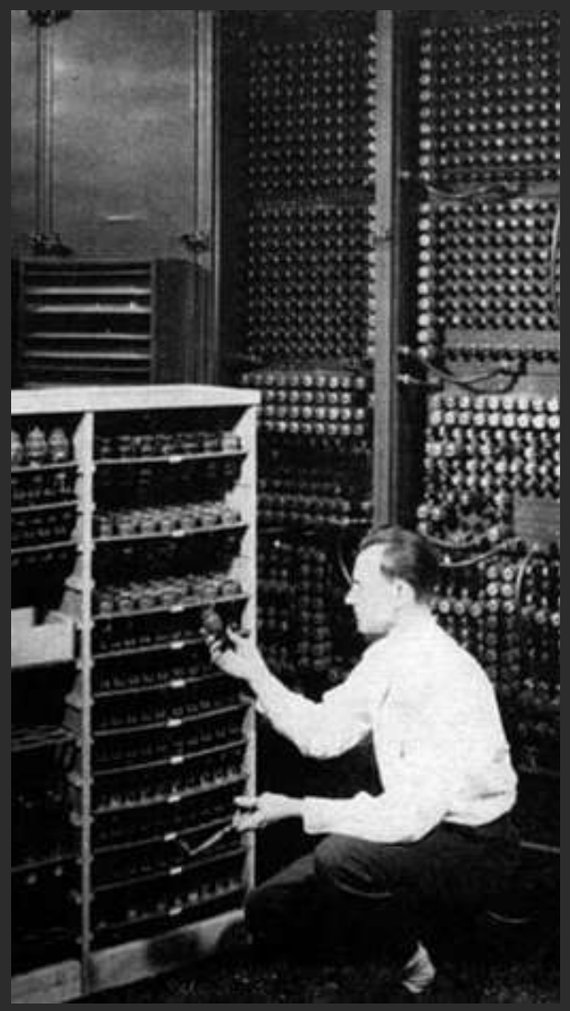
A quantum computer is one that utilises phenomena from quantum physics.

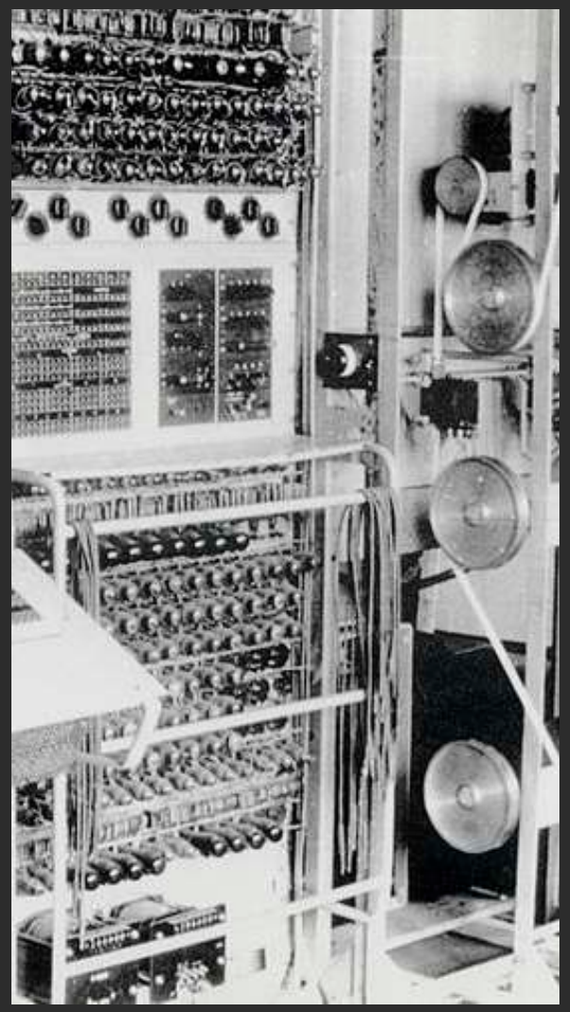
We all inhabit – and intuitively understand – a world governed by Newtonian physics – which explains the behaviour of tangible things such as billiard balls, planets and falling apples

However, Newton's laws do not apply at the scale of subatomic particles and so quantum theory evolved to explain the often strange behaviour of nature at the very small scale

Quantum computers make use of two particular features of Quantum Mechanics, that is superposition and entanglement

IBM’s new 53 Qubit Quantum Computer





EARLY CLASSICAL COMPUTERS

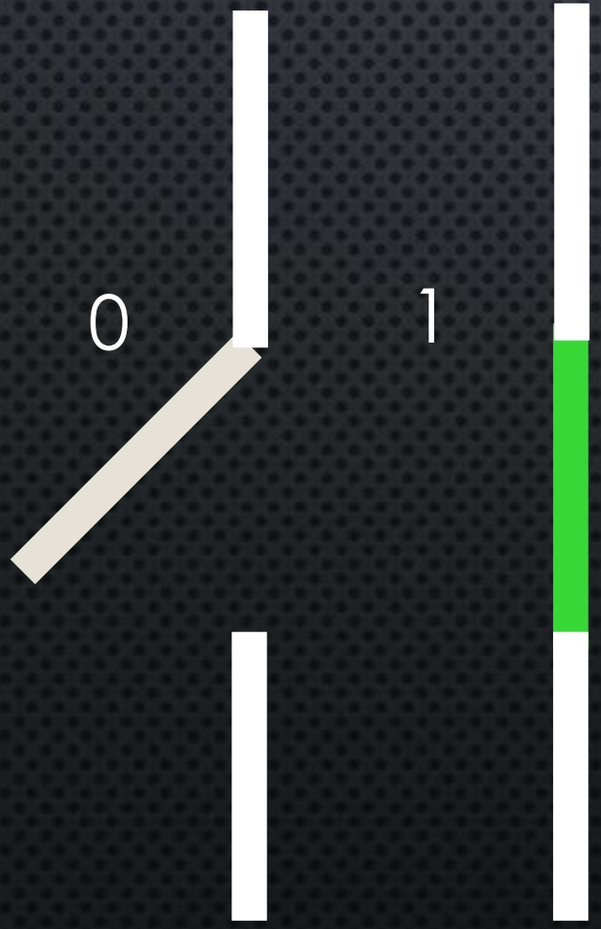
ABC, COLOSSUS AND ENIAC

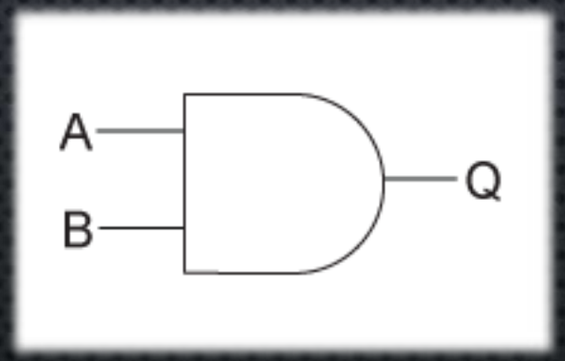
THE CONCEPT OF A STORED-PROGRAM COMPUTER WAS INTRODUCED IN THE MID-**1940S**, AND THE IDEA OF STORING INSTRUCTION CODES AS WELL AS DATA IN AN ELECTRICALLY ALTERABLE MEMORY
WAS IMPLEMENTED IN EDVAC (*E*LECTRONIC *D*ISCRET E VARIABLE AUTOMATIC COMPUTER)

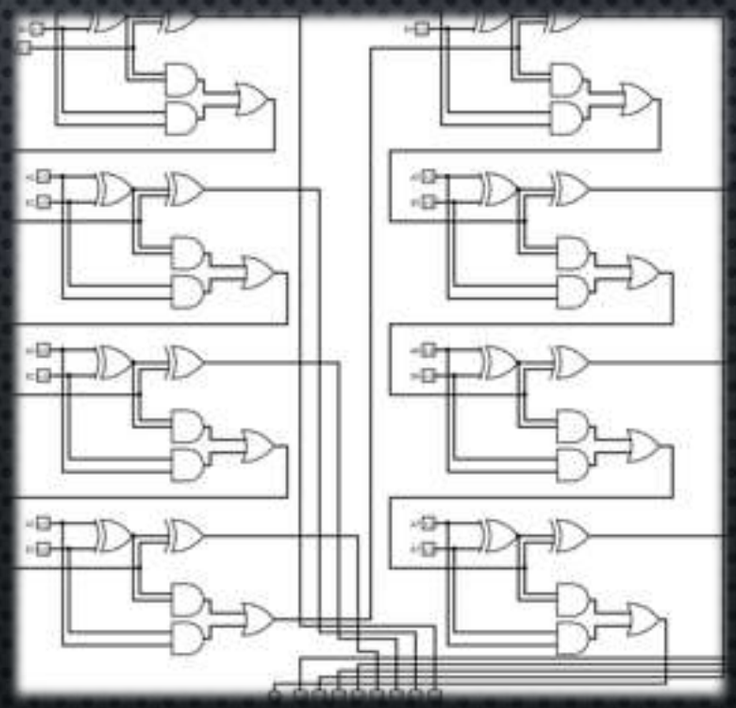
OPERATING SYSTEMS WERE INTRODUCED IN THE 1950S

Manchester Mark 1, the first stored program digital computer. c1949

HOW DIGITAL COMPUTERS WORK

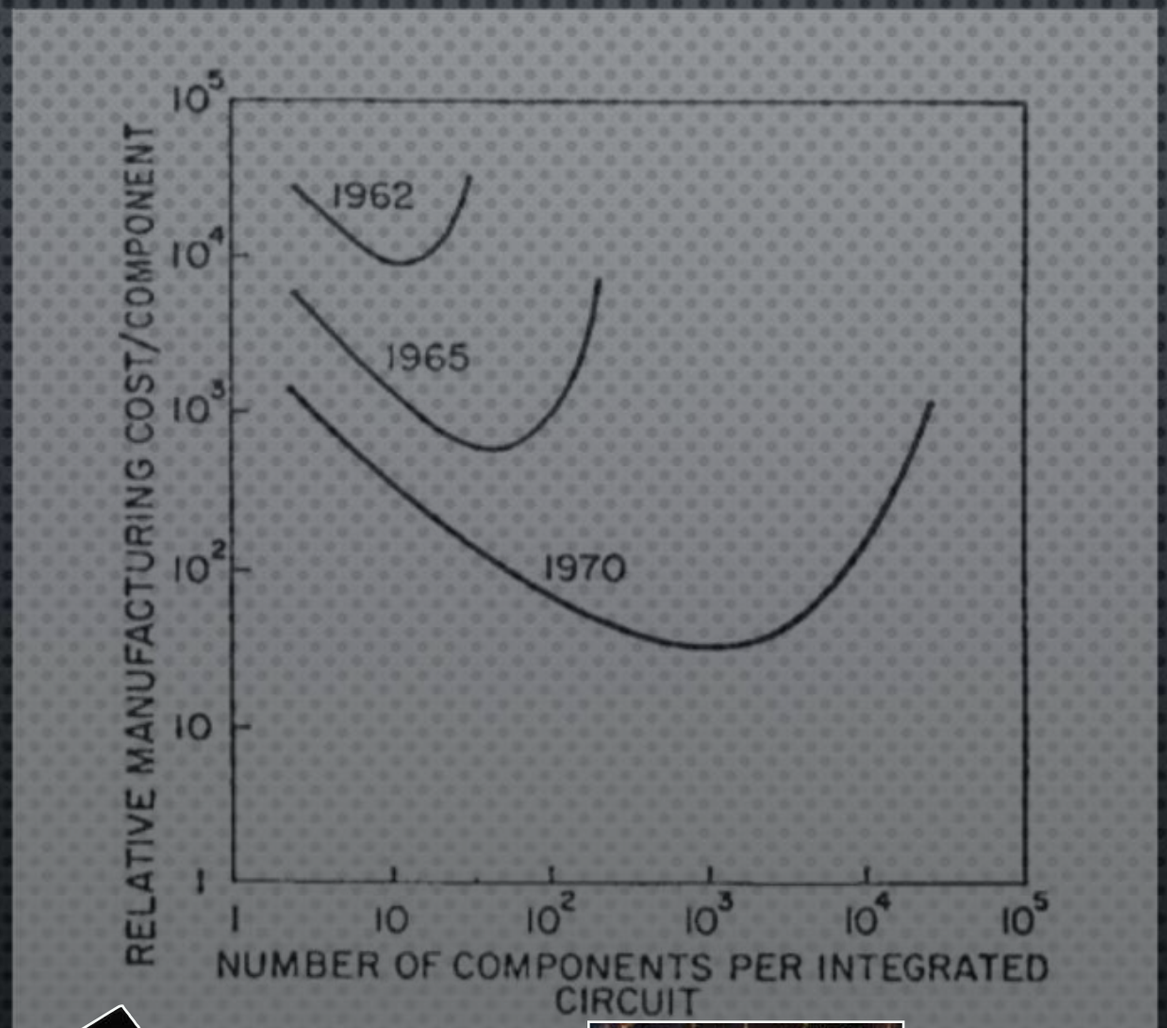


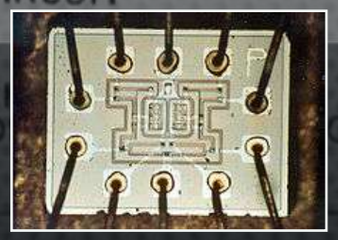


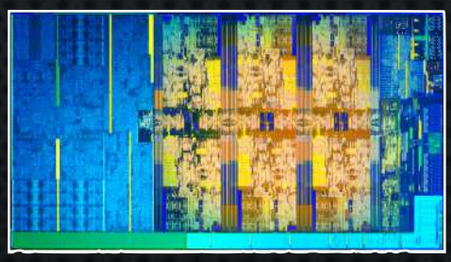


MOORE'S LAW

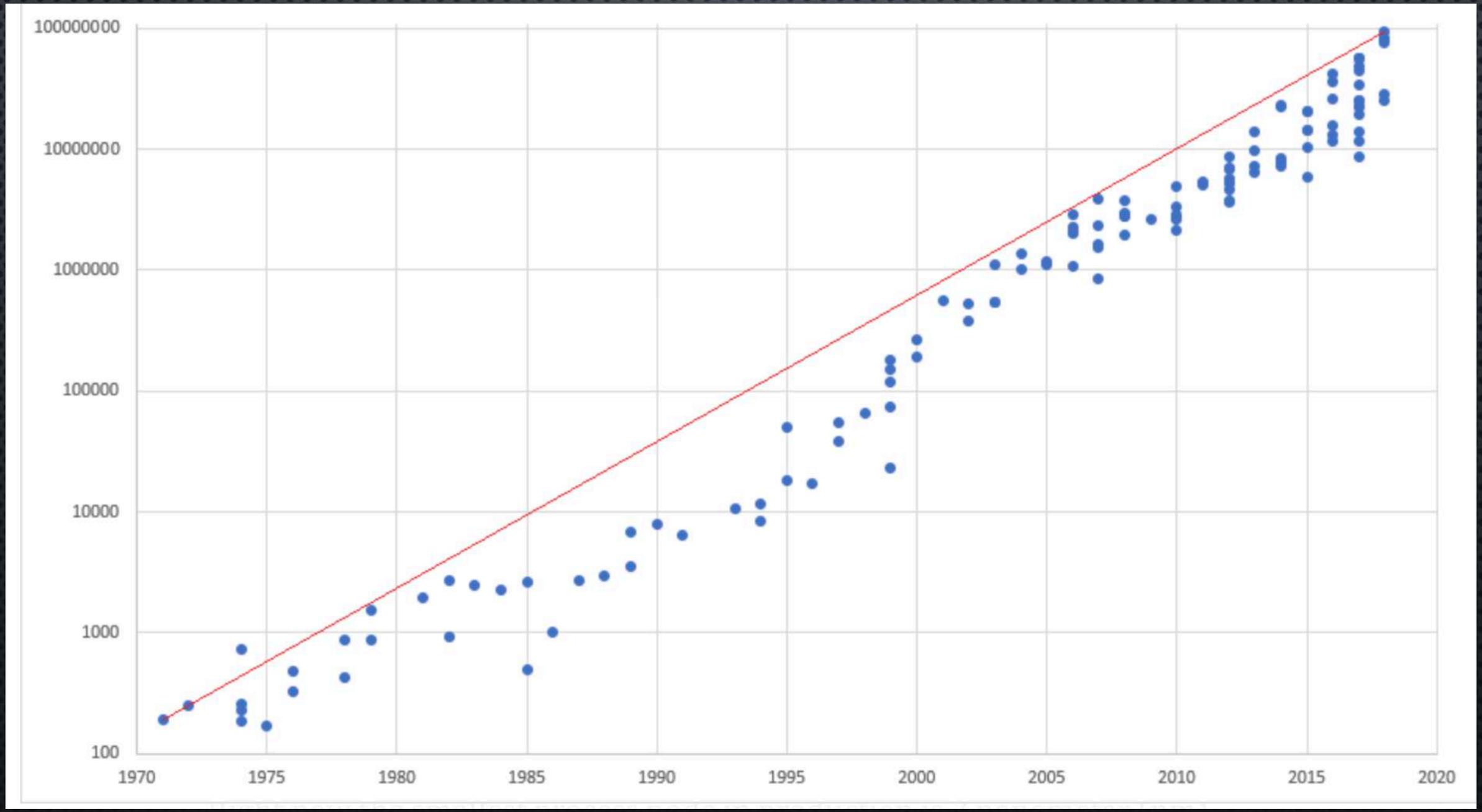
The number of transistors that can be installed on an integrated circuit roughly doubles every two years







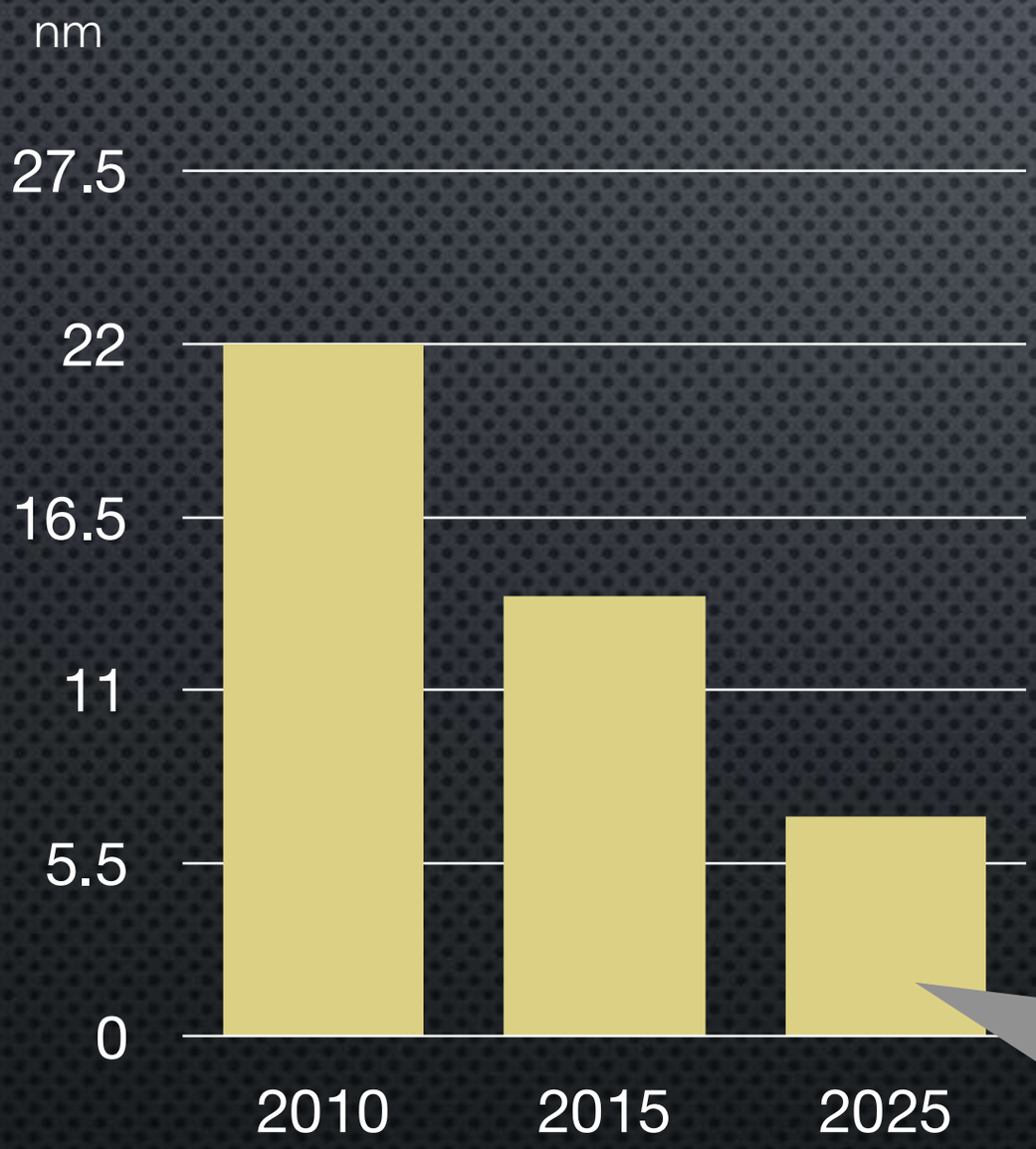
TRANSISTOR DENSITY 1971-2020 – SOURCE WIKI



WHY MORE TRANSISTORS HELP?

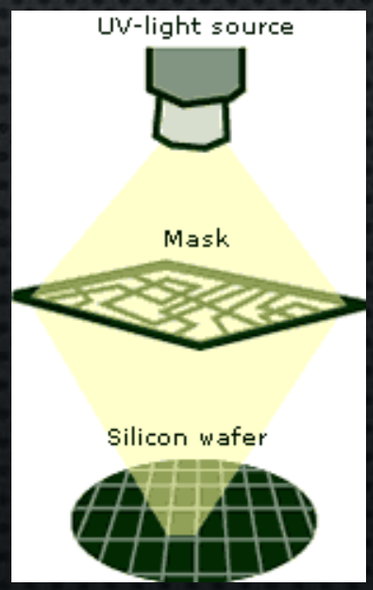
- From a programmer's point of view it looks sequential
- A great deal of parallel activity, large caches to reduce latency, reduce communication latency, more registers, more side tasks being performed, wider registers, more complex operations, pipelining
- So, more transistors are good as is multicore processors

THE END OF MOORE'S LAW?



"You canny change the laws of physics"

Probably reach maximum density here

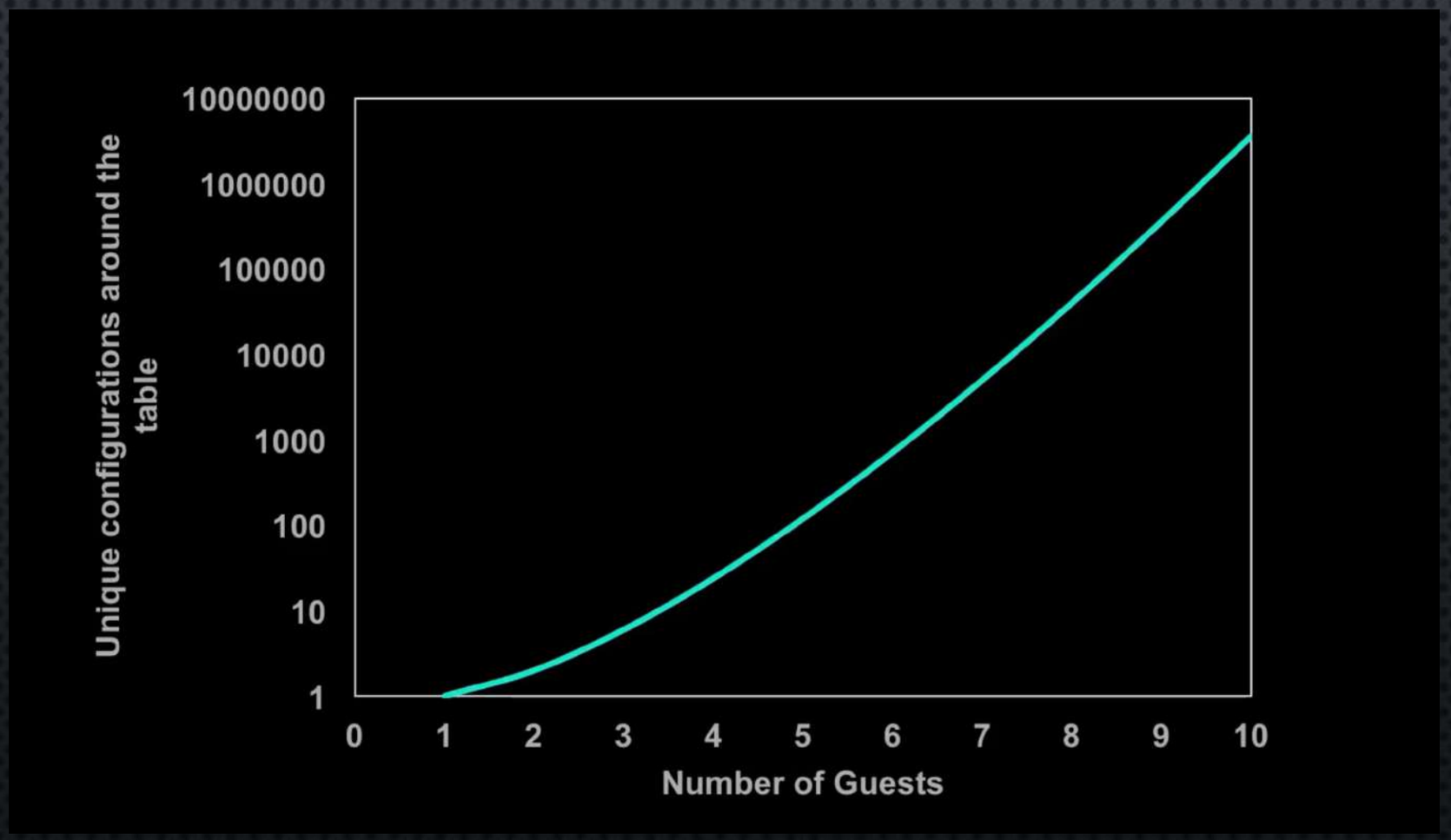


In 1980, 5 microns was typical

CHESS, A GO AND A WEATHER PREDICTION COMPUTER

Supercomputer, any of a class of extremely powerful computers

DINING GUEST PROBLEM

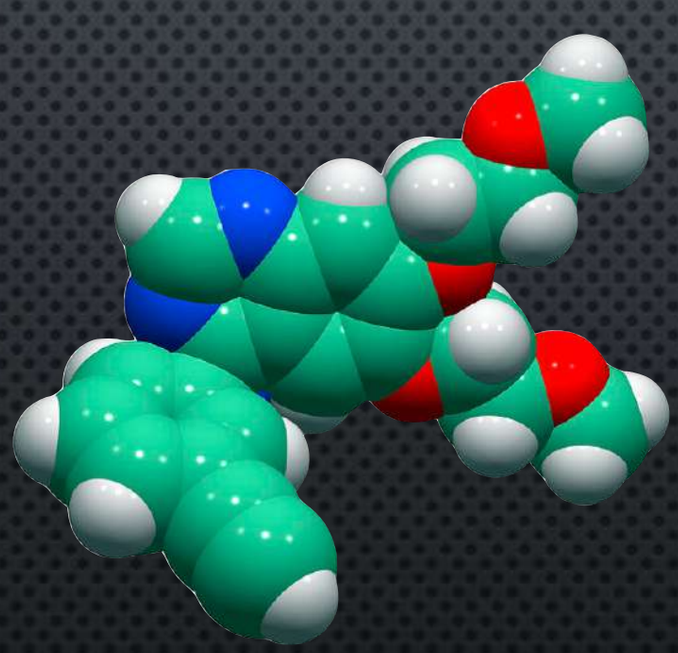


COMPUTATIONAL DRUG DESIGN

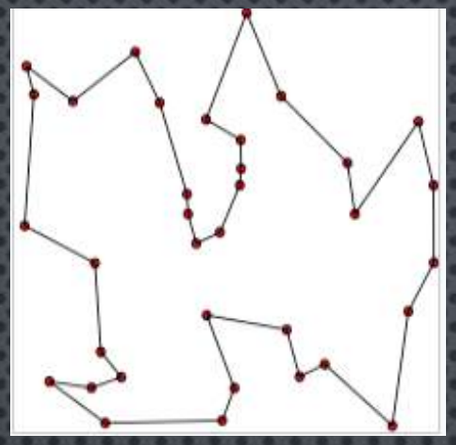
- The most fundamental goal in drug design is to predict whether a given molecule will bind to a target and if so how strongly
- For example, predicting how a cancer drug interacts with a tumor and other body cells is computationally a very difficult problem
- Currently requires approximations
- As such problems are in fact quantum mechanical

COMPUTATIONAL DRUG DESIGN

- EVEN WITH RELATIVELY SIMPLE MOLECULES, CLASSICAL COMPUTERS STRUGGLE WITH THIS TYPE OF SIMULATION, BECAUSE THE MEMORY REQUIRED GROWS EXPONENTIALLY



THE TRAVELLING SALESMAN PROBLEM



- GIVEN A LIST OF CITIES AND THE DISTANCES BETWEEN EACH PAIR OF CITIES, WHAT IS THE SHORTEST POSSIBLE ROUTE THAT VISITS EACH CITY EXACTLY ONCE AND RETURNS TO THE ORIGIN CITY?
- IN THE WORST CASE (WITHOUT HEURISTICS OR APPROXIMATIONS) THE RUNNING TIME FOR AN ALGORITHM INCREASE SUPERPOLYNOMIALLY
- IT IS A VERY USEFUL THING TO SOLVE FOR LOGISTICS BUT ALSO MICROCHIP MANUFACTURE, DNA SEQUENCING ETC
- THIS TYPE OF PROBLEM IS KNOWN AS AN NP-COMPLETE PROBLEM

WHAT ARE DIGITAL COMPUTER NO GOOD AT?

- COMBINATIONAL **OPTIMISATION** PROBLEMS – SUCH AS THE TRAVELLING SALESMAN – THESE HAVE EXPONENTIALLY POTENTIAL SOLUTIONS
- THESE PROBLEMS ARE CHALLENGING FOR STANDARD COMPUTERS, EVEN SUPERCOMPUTERS, BECAUSE AS THE PROBLEM SIZE GROWS, AT SOME POINT, IT TAKES THE AGE OF THE UNIVERSE TO SEARCH THROUGH ALL THE POSSIBLE SOLUTIONS!
- IF AT ALL POSSIBLE, THESE PROBLEMS ARE WORTH SOLVING WITHOUT RESORTING TO ALL SORTS OF APPROXIMATIONS

WHAT CLASSICAL COMPUTERS CAN AND CANNOT DO

- A COMPUTER SCIENTIST WE CLASSIFY PROBLEMS ACCORDING TO HOW MANY COMPUTATIONAL STEPS IT TAKES TO SOLVE A LARGE EXAMPLE OF THE PROBLEM USING THE BEST ALGORITHM KNOWN

- **P PROBLEMS** – THESE PROBLEMS CAN BE SOLVED EFFICIENTLY IN POLYNOMIAL TIME FOR EXAMPLE A PROBLEM WITH N INPUTS REQUIRES A NUMBER OF STEPS IS PROPORTIONAL TO N^2

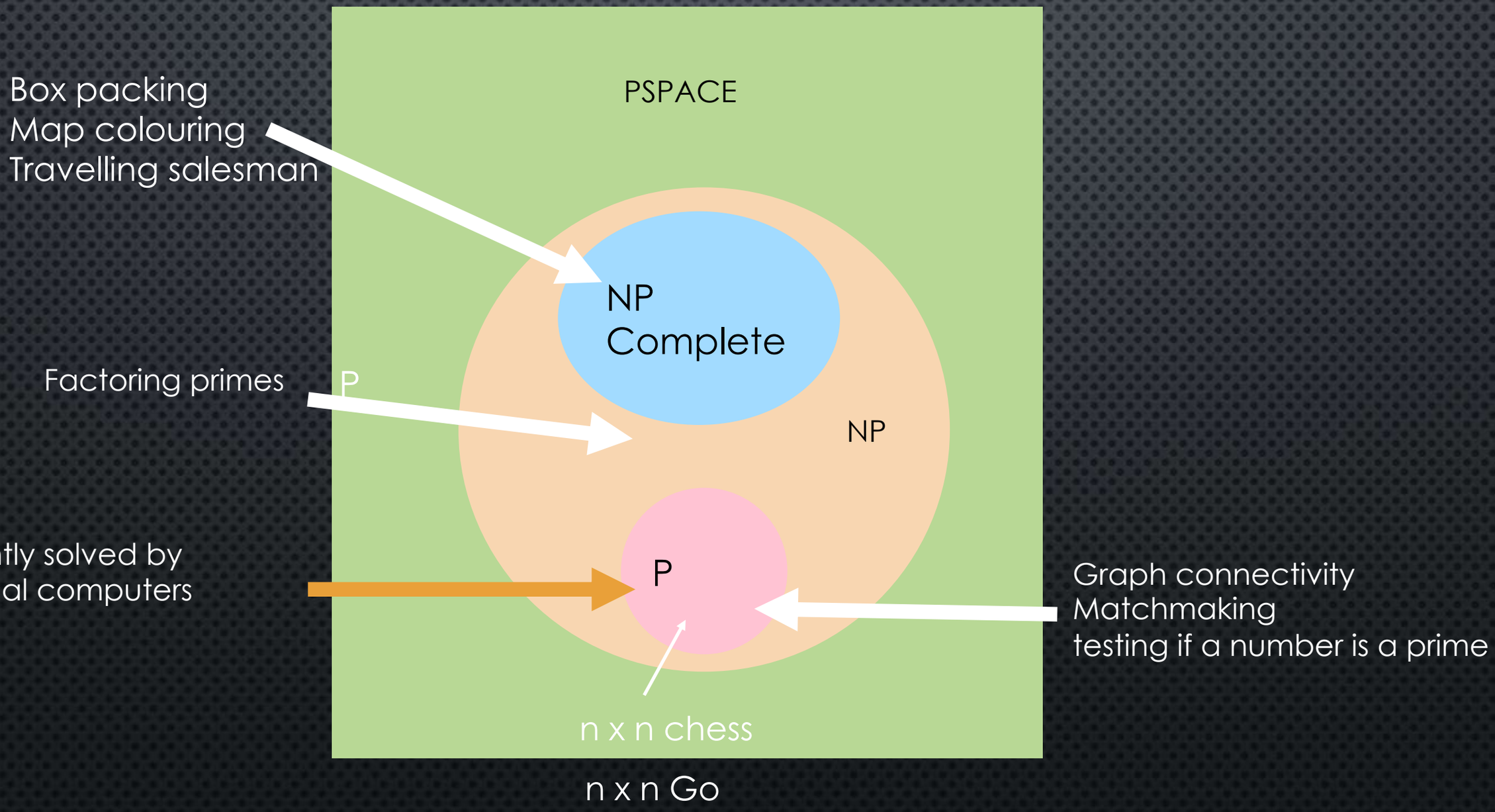
- **NP PROBLEMS** EASY TO VERIFY, FOR EXAMPLE, YOU KNOW AN N DIGIT NUMBER IS PRODUCT OF TWO LARGE PRIMES AND YOU WANT TO FIND THE PRIME FACTORS. IF YOU KNOW THE FACTORS IT IS SIMPLE TO VERIFY IN POLYNOMIAL TIME

- THE PROBLEM IS SOLVING THESE, AS NO KNOWN ALGORITHMS FOR A CLASSICAL COMPUTER IN POLYNOMIAL TIME, INSTEAD THE STEPS GET EXPONENTIALLY BIGGER

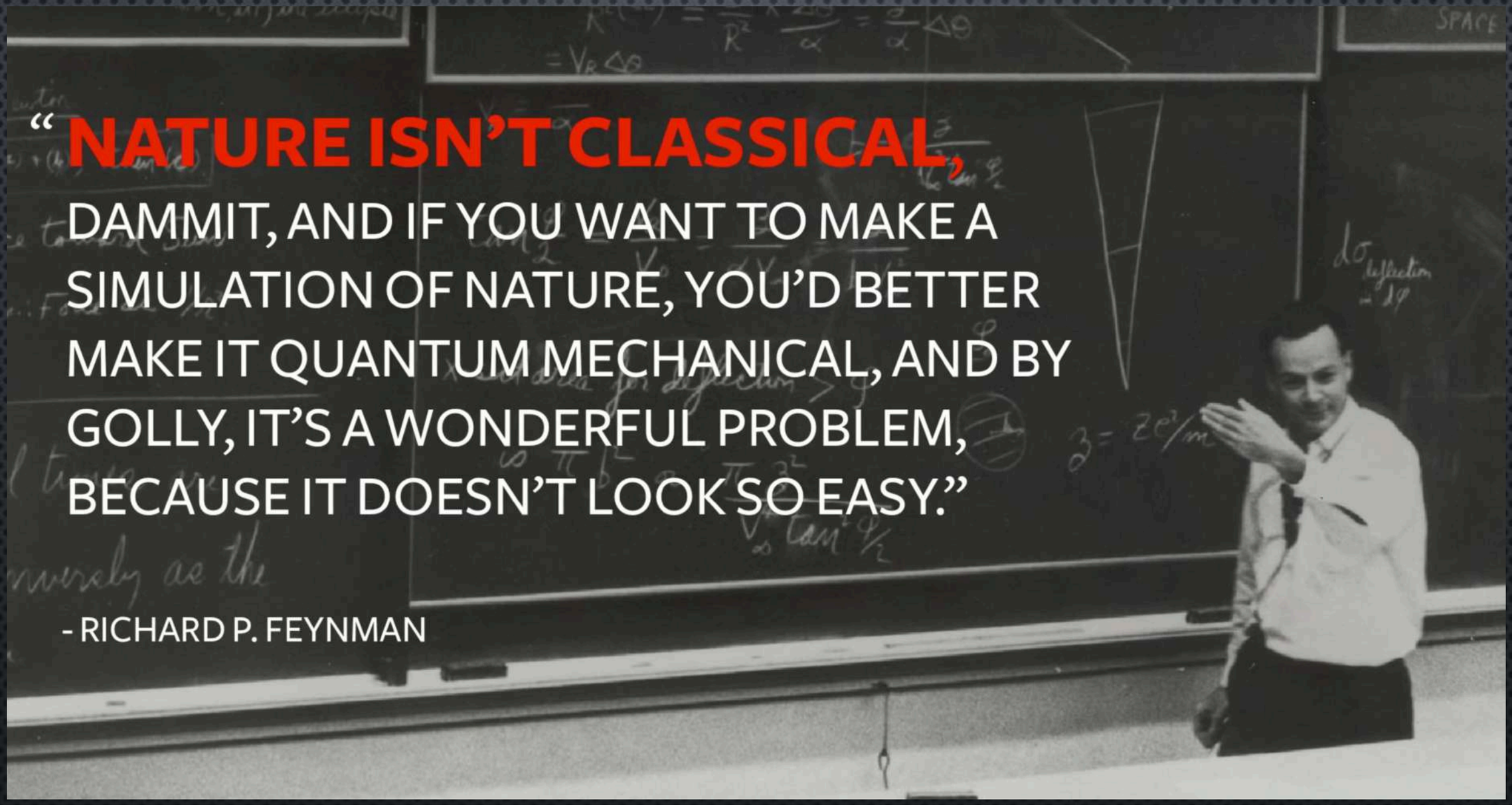
NP COMPLETE

- An efficient solution to one would provide an efficient solution to all NP challenges
- Map problems - can you colour any map's countries with just 3 colours without any two bordered countries being the same colour? No known algorithm's can solve NP complete problems efficiently

PSPACE


Box packing
Map colouring
Travelling salesman
PSPACE
NP
Complete
Factoring primes
P
NP
Efficiently solved by
classical computers
P
Graph connectivity
Matchmaking
testing if a number is a prime
n x n chess
n x n Go

QUANTUM COMPUTING

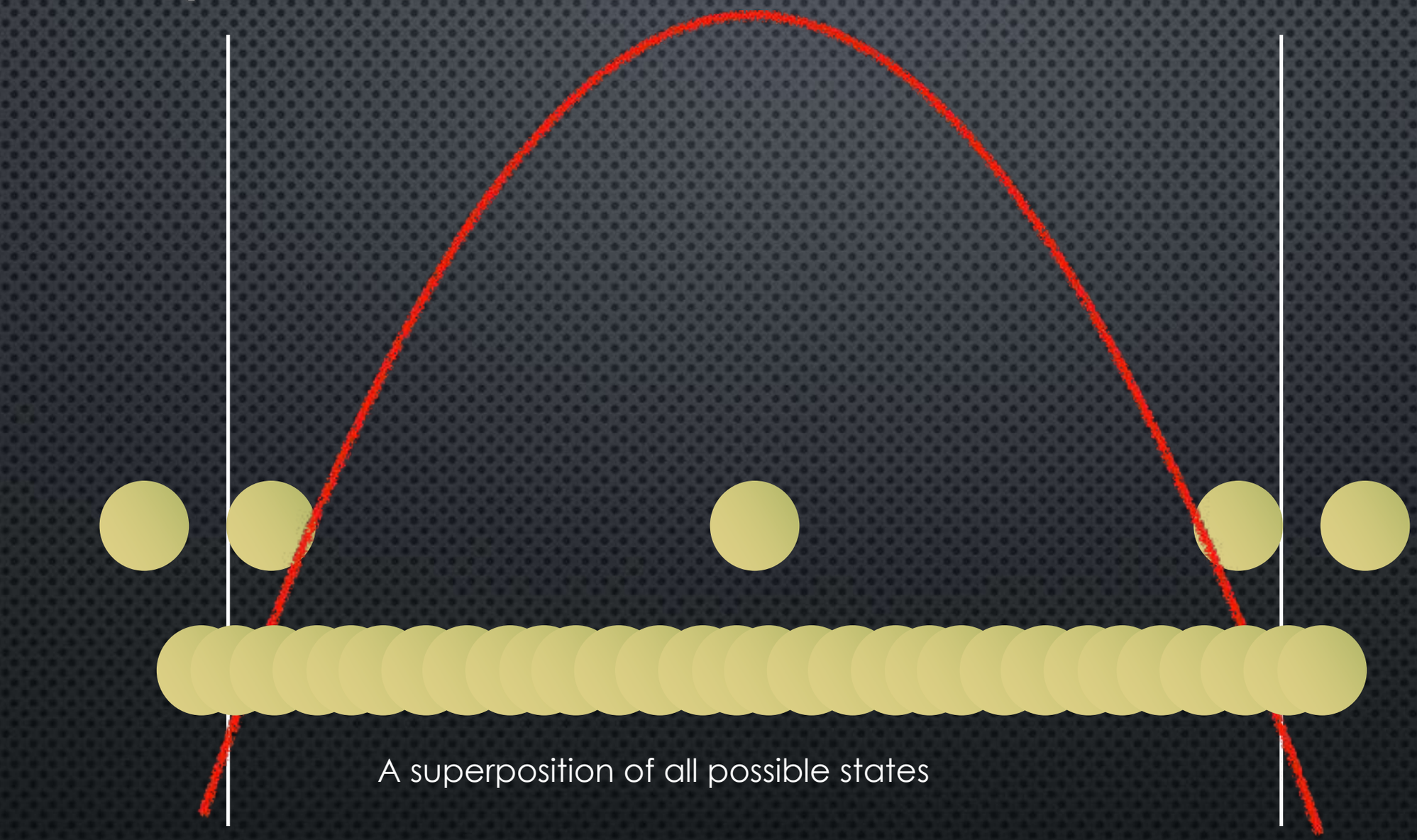


“If you think you understand quantum mechanics, you don’t understand quantum mechanics.”

Quantum Mechanics

- Quantum mechanics is relatively new (last 150 years)
- It was discovered when classical Physics (particularly when studying light) simply stopped working for certain problems
- It turns out that the world we observe only doesn't appear to behave in classical manner because of the Scale of everyday objects
- However, at the Atomic scale everything is different and matter blurs into probability waves and particles are both waves and particles
- Quantum theory works brilliantly and helps us design amazing technology

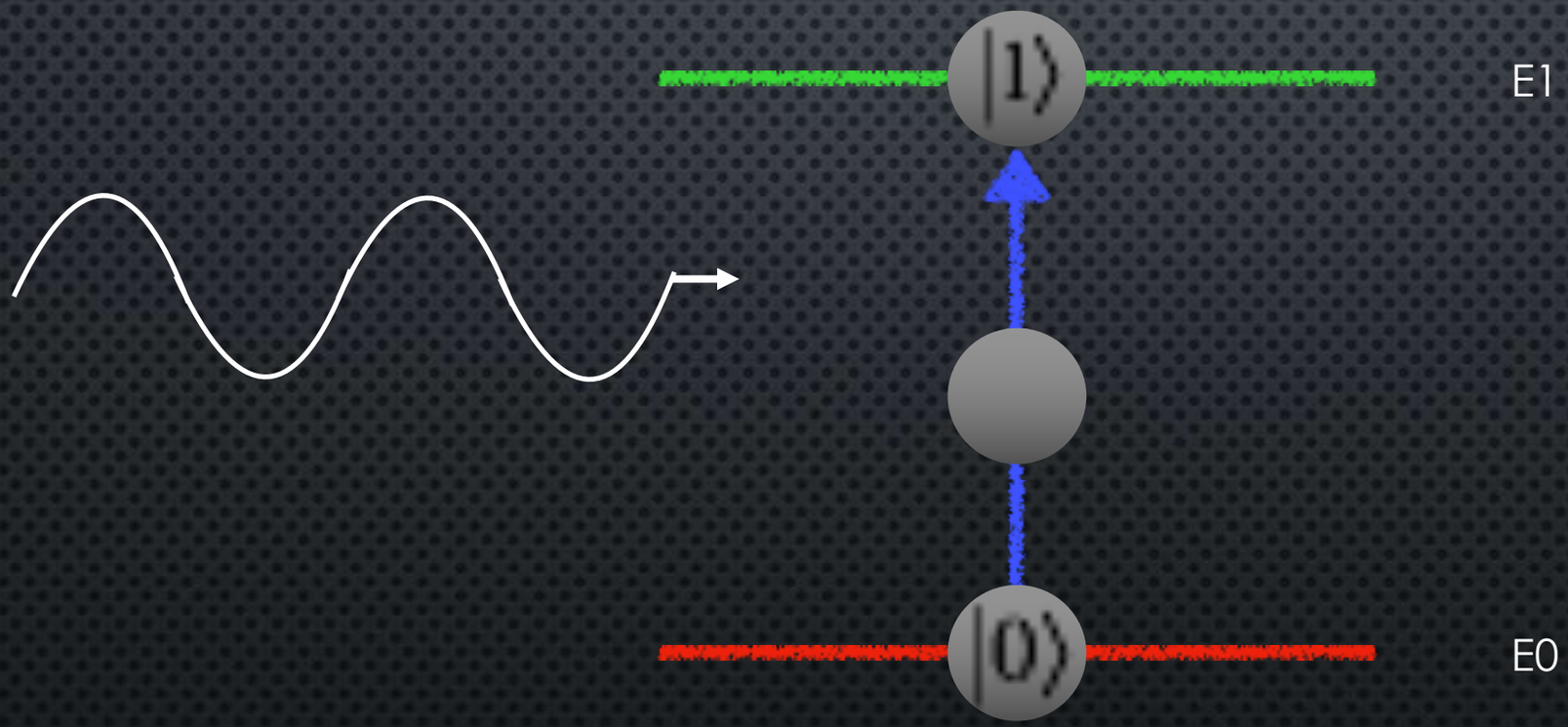
THE QUANTUM WORLD



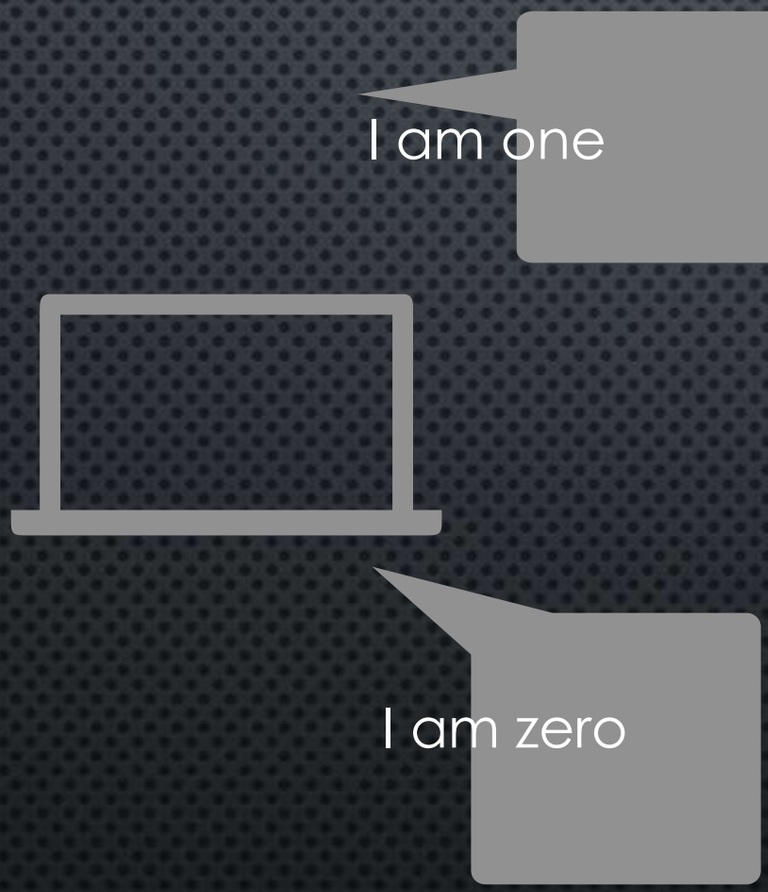
A superposition of all possible states

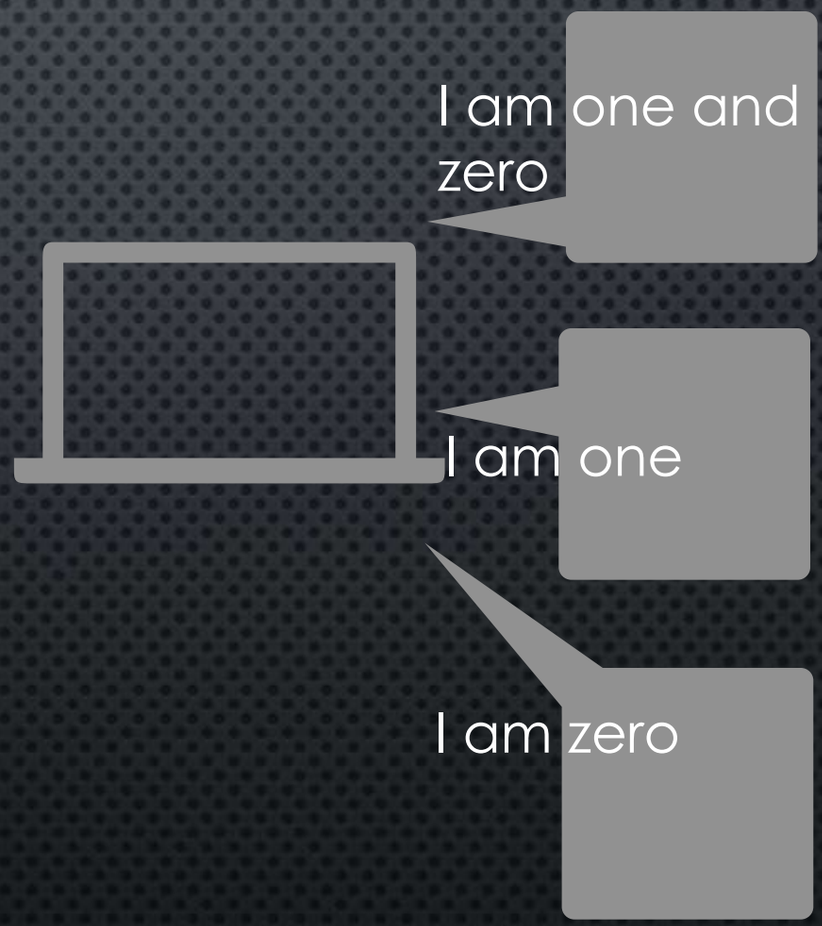
THE QUANTUM WORLD

THE QUANTUM BIT



CLASSICAL AND QUANTUM BIT

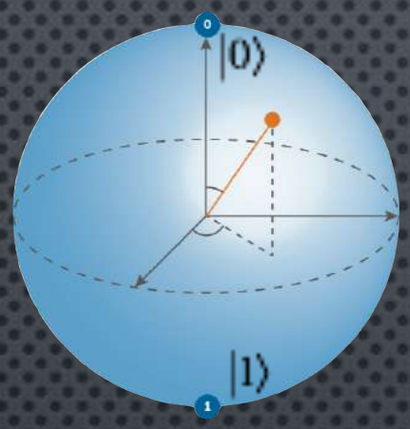


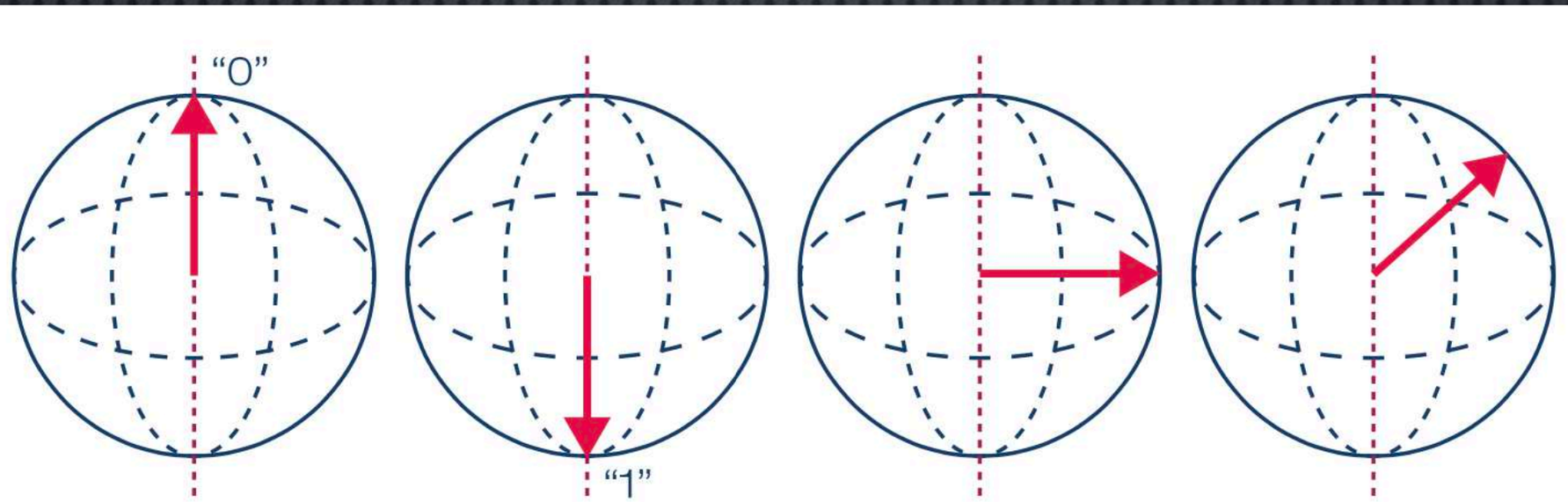


Not a replacement

quantum computing as a cloud service
np complete problems

THE QUBIT – THE QUANTUM VERSION OF THE CLASSICAL BIT – THE BLOCH SPHERE





Left to right: qubit in state “0”, qubit in state “1”, qubit in superposition with 50% probability of measuring “0” or “1”, qubit with higher probability to retrieve “0” than “1”.

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$$

CLASSICAL VS QUANTUM BITS

Classical 2 bits = 3 states (0,1,2)
Classical 8 bits = 256 states (0-255)

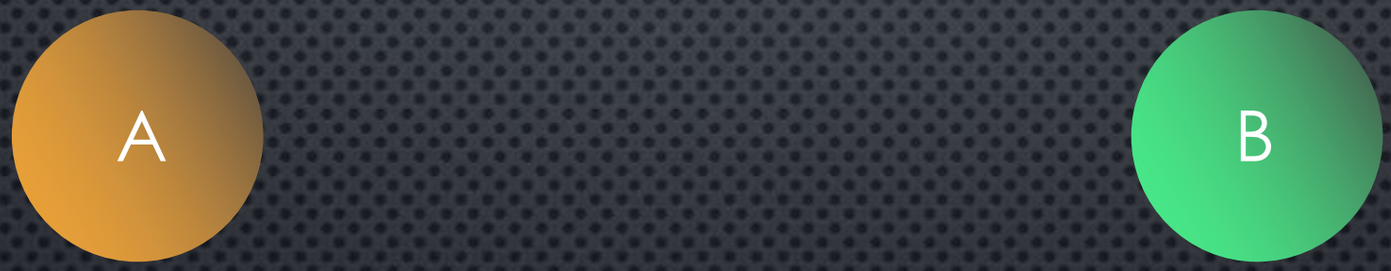
64 qubits = 18,446,744,073,709,600,000

This is millions of terabytes

QUANTUM ENTANGLEMENT

State of A
depends on the state of B

State of B
depends on the state of A



System is in state C which is dependent of the state of A and B

State is: position, momentum, spin, and polarisation

ENTANGLEMENT SPINNING COIN ANALOGY

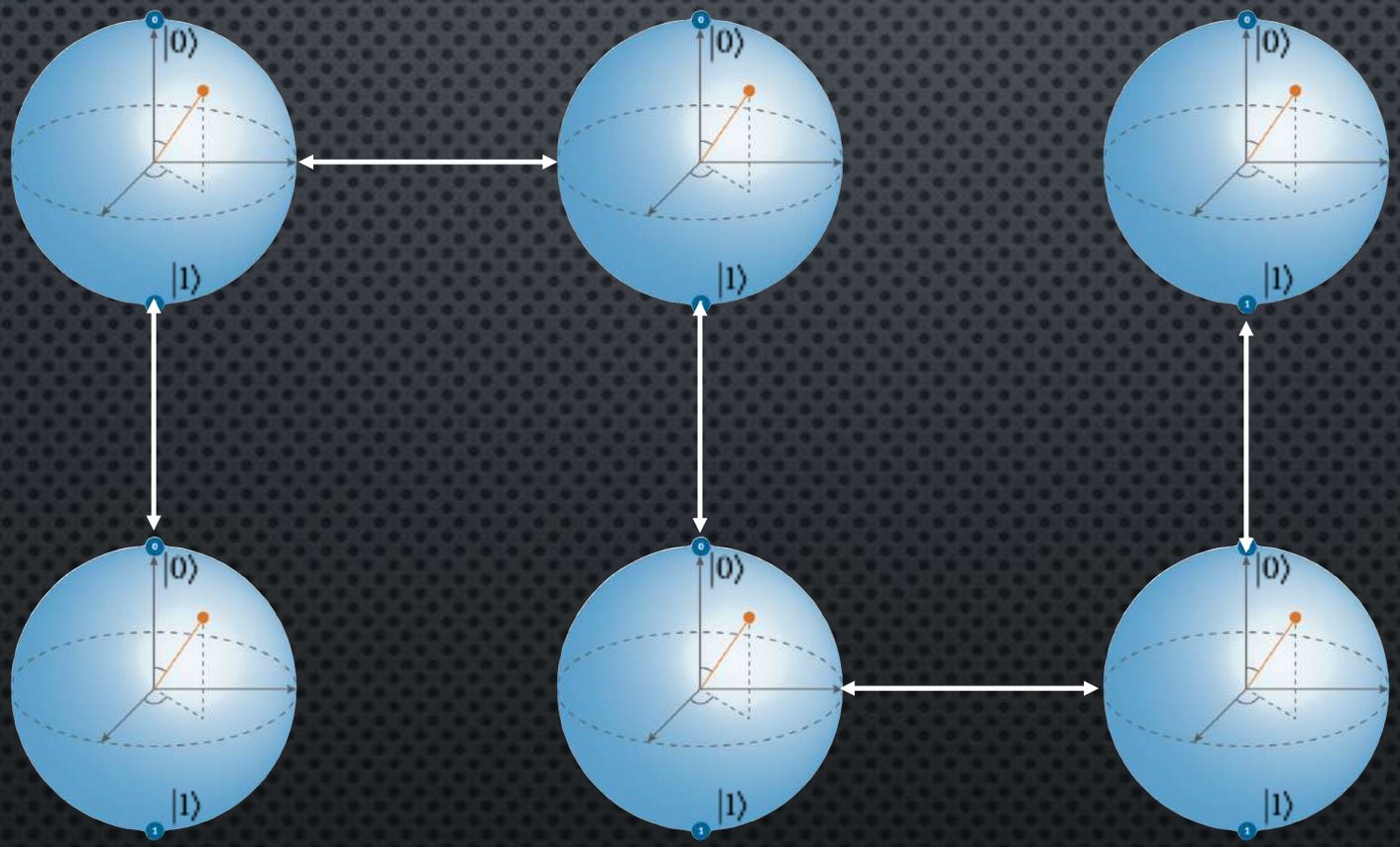
2.5 million light years

If one land on heads the other will land on heads

If one land on tails the other will land on tails

It does not matter how far they are apart - one could be in the next galaxy

WE CAN ENTANGLE QUBITS TO MAKE GATES

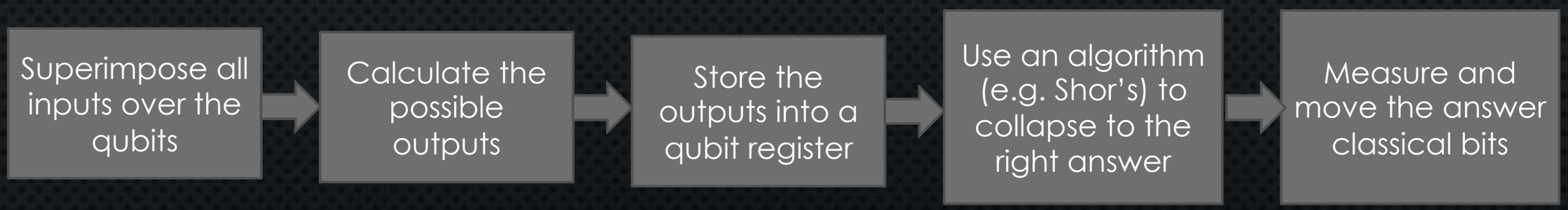


QUBIT REGISTER

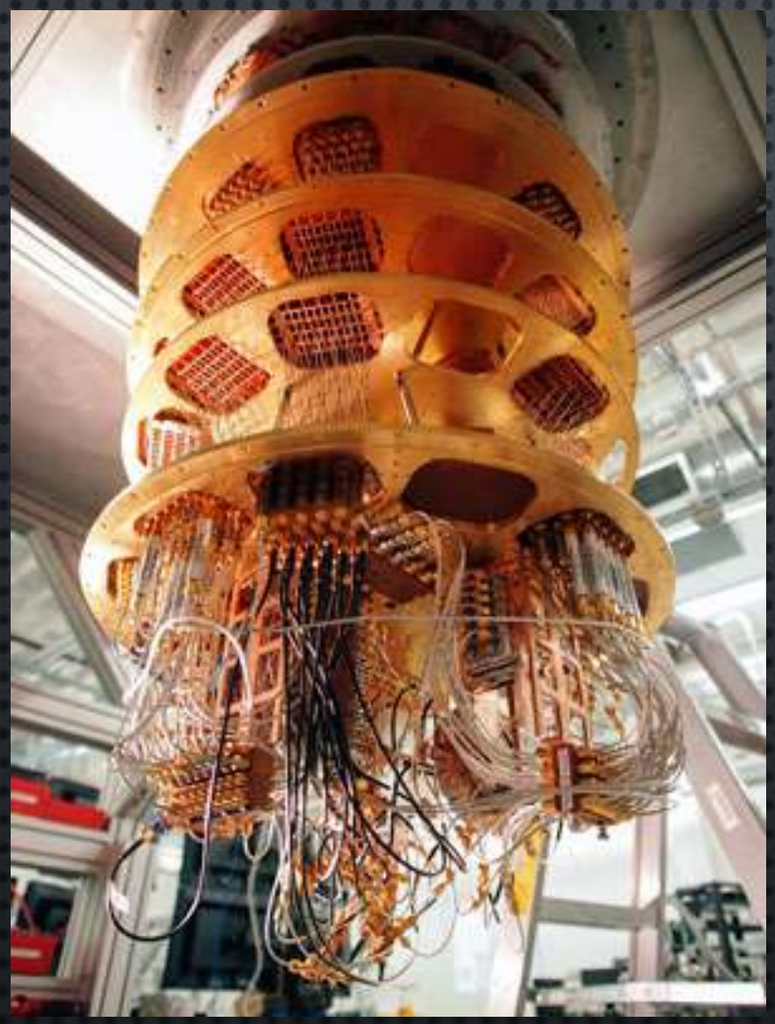
- A COMBINATION OF SEVERAL QUBITS IS CALLED A QUBIT REGISTER
- QUANTUM ALGORITHMS WORKING ON QUBIT REGISTERS PRESERVE THEIR SUPERPOSITION STATE THROUGHOUT THE CALCULATION
- WHEN THE ALGORITHM IS FINISHED, A MEASUREMENT IS CONDUCTED AND A RESULTING BITSTRING COMPOSED OF “0”S AND “1”S IS READ OUT FROM THE QUBIT REGISTERS.

Operation

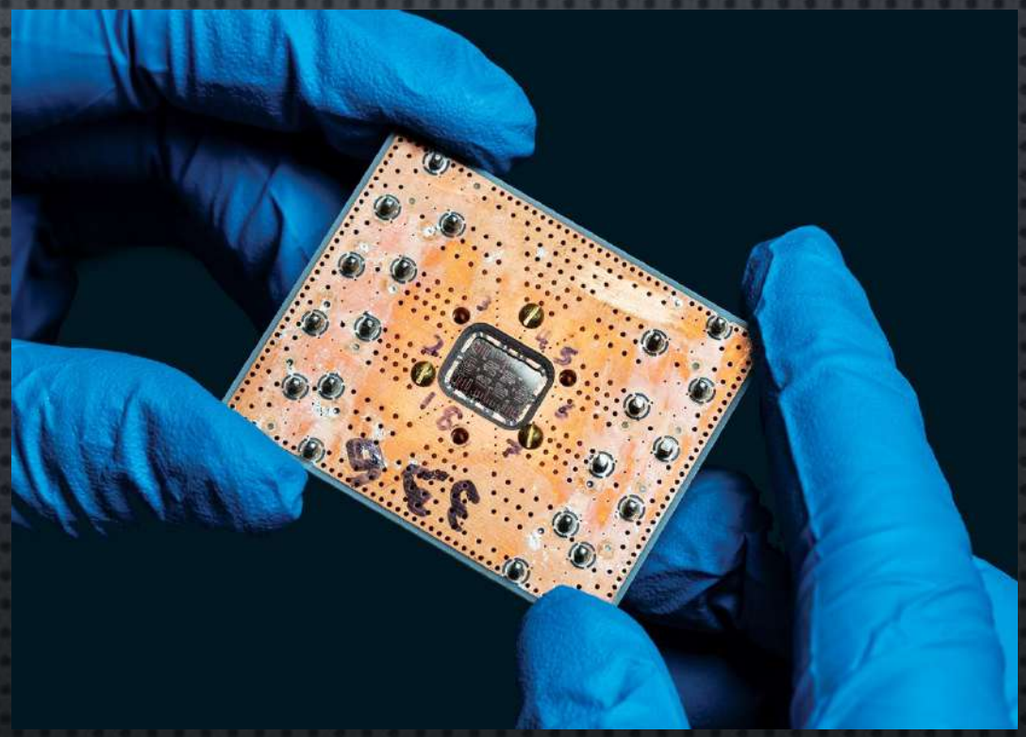
- Think of the task of finding an input value that leads to a specific output value: on a classical computer, the corresponding algorithm has to be repetitively executed for different inputs until the Solution is found
- On a quantum register can hold all possible input values at once by encoding them in superposition states
- A quantum algorithm capable of working with such a quantum register calculates the corresponding output and stores it in another quantum register
- This output is not a single bitstring, but again a superposition of states. In this case: the superposition of all possible outputs
- So far, the quantum computer has not yet solved the search problem, as reading out the results register will give a numbers of the potential results with a certain probability
- The "correct" result can be selected in a Sophisticated way using an algorithm, cancelling out the probability of measuring an incorrect result eventually leading to the correct results such as the two primes used to generate an encryption key



QUANTUM COMPUTING

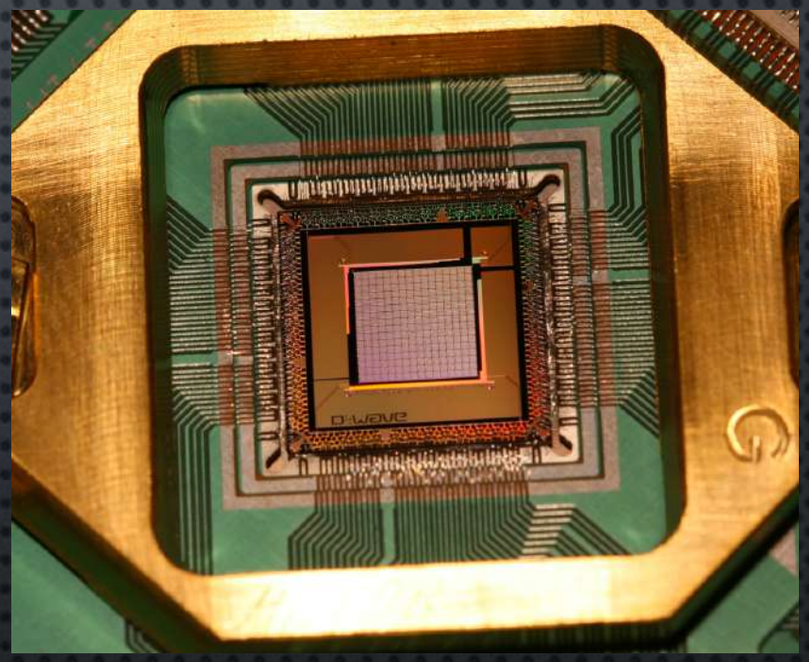


Google has 9 qubit now and planning a 50 bit



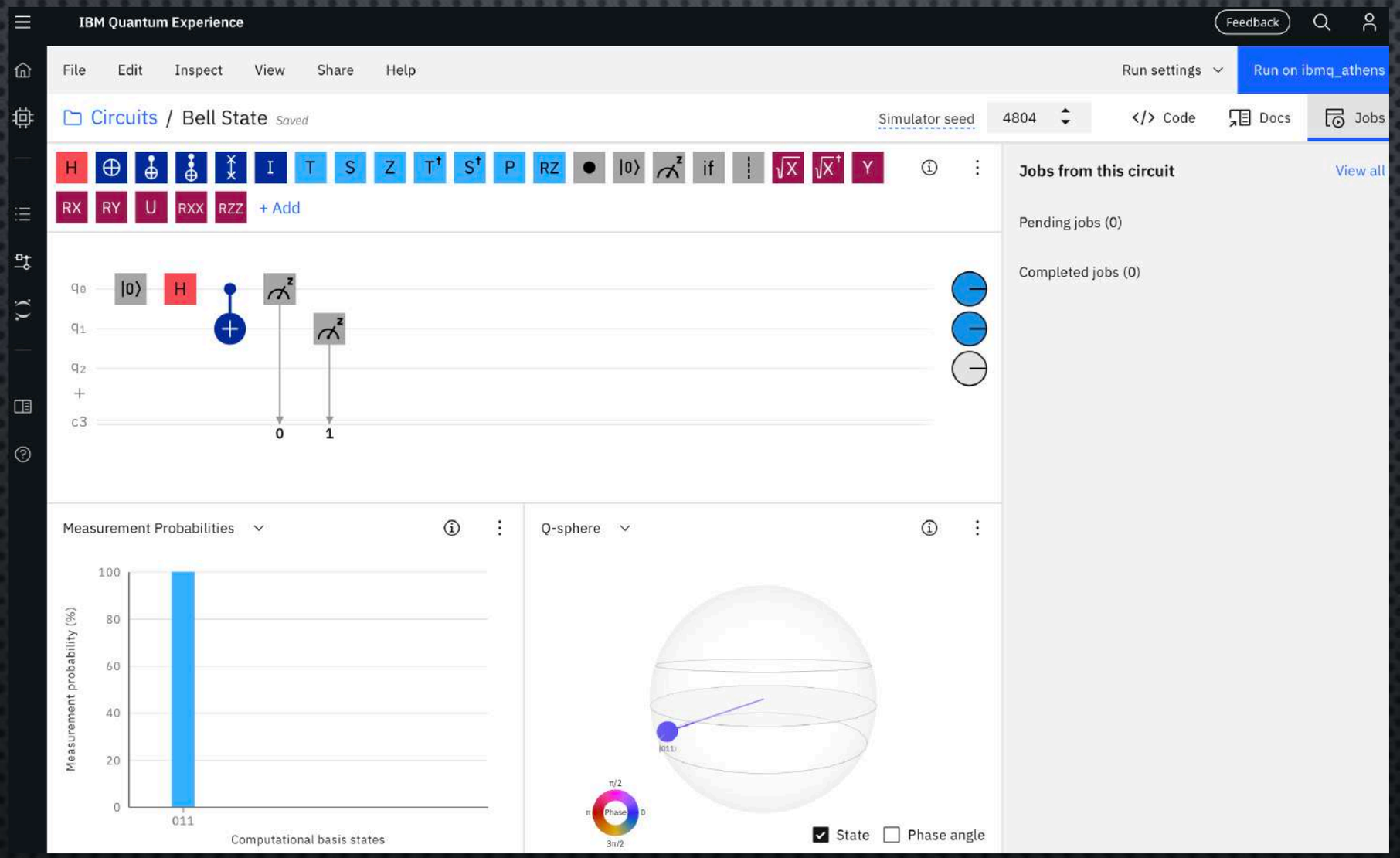
IBM has working 5 qubit systems and beta access to a 16 qubit system

D - WAVE - QUANTUM ANNEALING



Google and NASA own one of these and they cost $15,000,000

IBM QUANTUM EXPERIENCE



PROGRAMMING ABSTRACTION

Classical	Quantum
Programming Frameworks	???
Operating System	???
Logic Gates	Gates
Bits	Qubits

TYPES OF PROBLEMS

- Machine Learning – training neural networks, recognising patterns
- Security - factoring integers, detecting viruses and network intrusion
- Financial Modelling - detecting market instabilities, portfolio optimisation
- Healthcare and Medicine - detecting fraud, creating protein models, generating drugs

SECURITY

- SHOR'S ALGORITHM CAN SOLVE BIG PRIME FACTOR AND CRACK AND FACTORING ENCRYPTIONS (RSA) – GIVEN ENOUGH QUBITS (THOUGH PROBLEM IS DECOHERENCE)
- FUTURE QUANTUM COMPUTERS WILL BE VERY GOOD AT THIS
- SO IN THEORY IT COULD CRACK ALL RSA PASSWORDS
- BUT – NO QUANTUM COMPUTER HAS ENOUGH QUBITS SO THIS MIGHT TAKE YEARS, ALSO THERE ARE OTHER ENCRYPTION TECHNIQUES - POST QUANTUM CRYPTOGRAPHY

NEW AGE OF COMPUTING?

- YES IT REALLY IS
- MANY TECHNICAL HURDLES TO OVERCOME BUT AS MORE INVESTMENT GOES IN IT BECOMES MORE AND MORE VIABLE
- ISSUES WITH PROGRAMMING QUANTUM COMPUTERS THOUGH LEVELS OF ABSTRACTION WILL OCCUR TO MAKE THIS MUCH EASIER TO 'CODE' THESE COMPUTERS
- DESKTOP QM COMPUTERS? PROBABLY NOT AS THESE ARE VERY SPECIALISED TO CERTAIN PROBLEMS SO MORE LIKELY TO BE A CLOUD SERVICE
- REPLACE CLASSICAL DIGITAL COMPUTERS? – NO AS THIS ARE HIGHLY OPTIMISED MACHINES AND PERFECT FOR MOST COMPUTING TASKS

HOW TO FIND OUT MORE

- IBM QUANTUM EXPERIENCE GIVES YOU THE OPPORTUNITY
- THERE ARE JOBS EVEN NOW FOR EXPERIENCED COMPUTER SCIENTISTS
- OPPORTUNITIES TO BE A PIONEER

END OF THE LECTURE

- Please note that there will be an accompanying question and answer session for this lecture