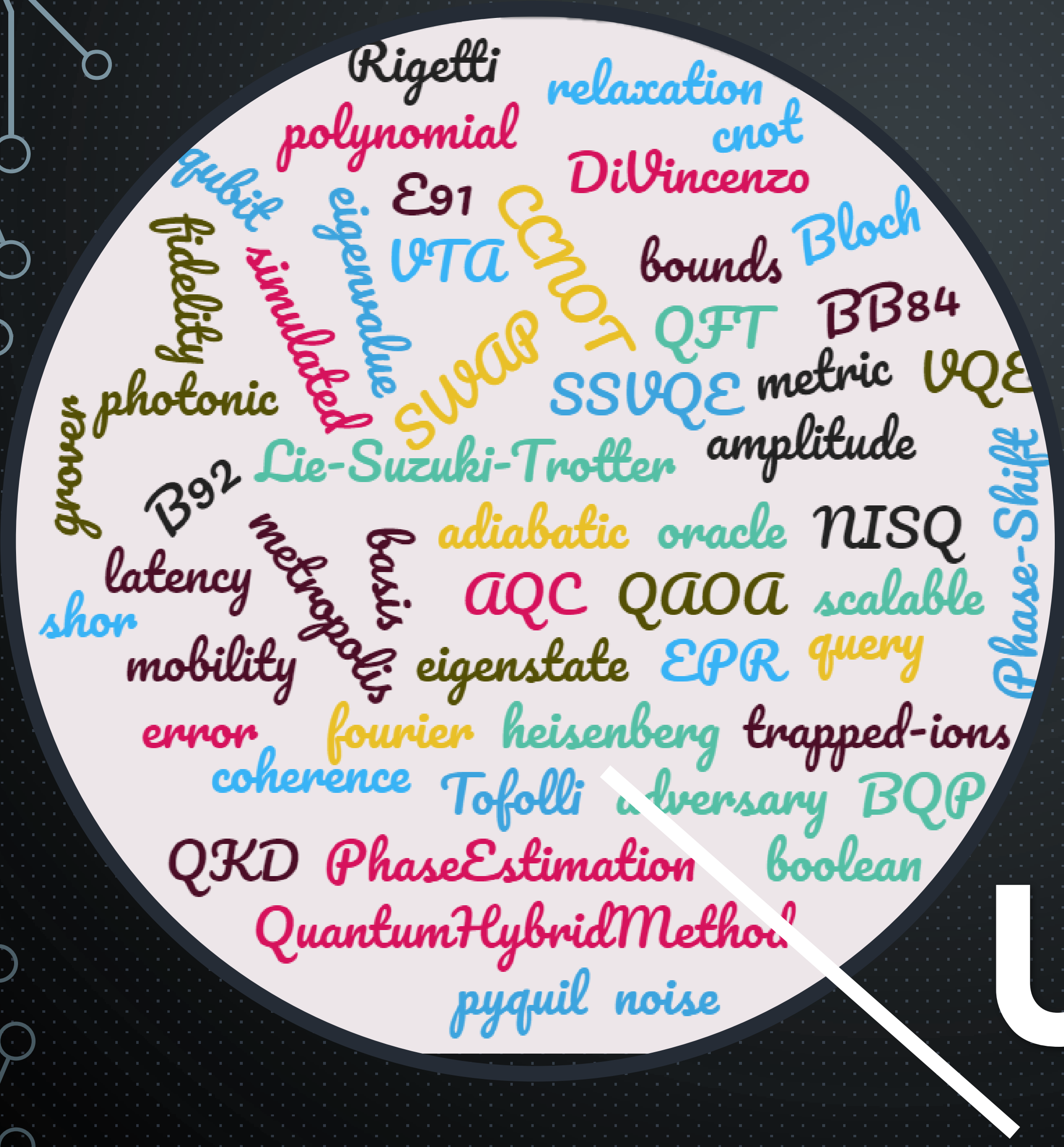


UANTUM

COMPUTING

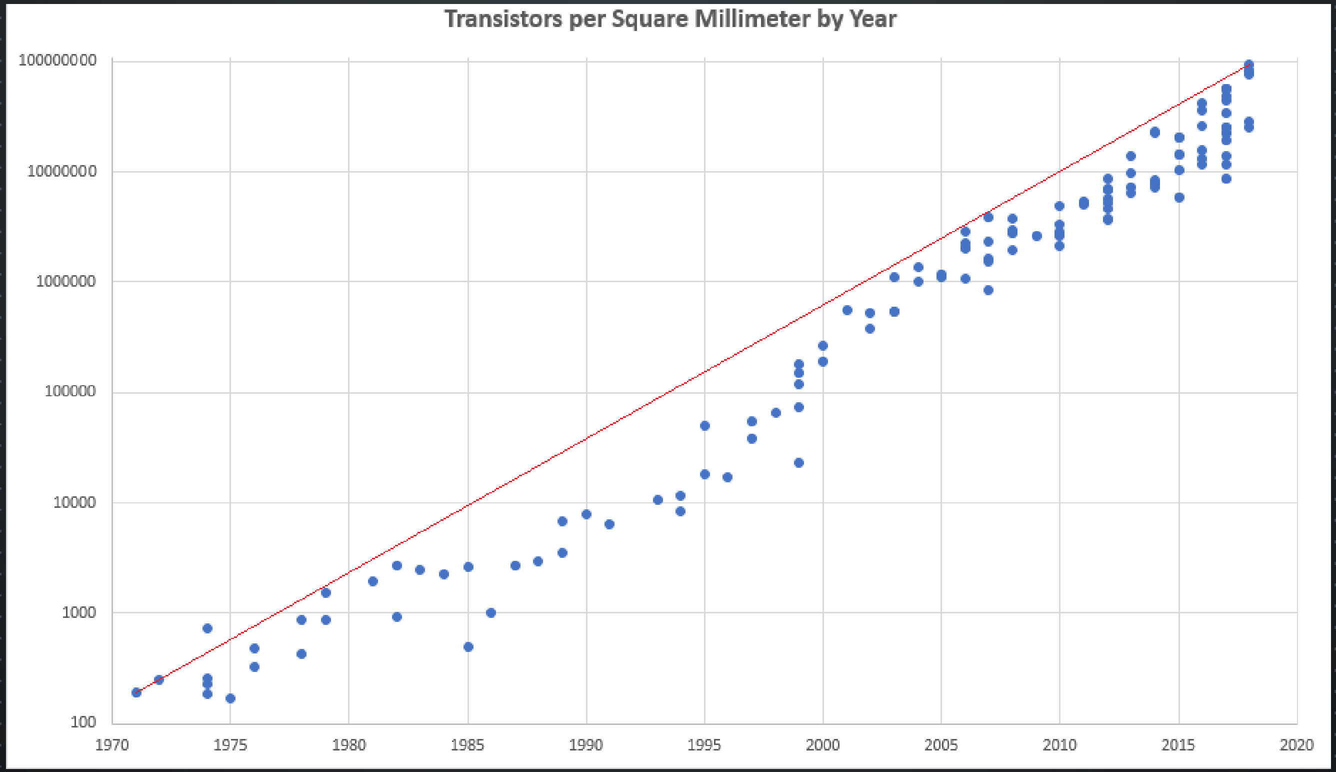
"Classical computation is like a solo voice - one line of pure tones succeeding each other. Quantum computation is like a symphony - many lines of tones interfering with one another" - Seth Lloyd

QUESTION TO PONDER ?

Classical computers have been around a long time, and in fact have only gotten faster with time. So what's the big deal about quantum computers? Why not build a faster classical computer? It seems to have worked out so far!

I. PROBLEMS WITH CLASSICAL COMPUTING

MOORE'S LAW



is an observation named after Gordon Moore (the co-founder and chairman emeritus of Intel). In 1965, Moore described a trend in which the number of transistors double on chips every two years. The observation has mostly held true, and as a consequence, the transistors on chips have been getting smaller and smaller. So much so that, they are now approaching sub-atomic sizes. At such sizes, quantum effects such as "electron tunneling" start becoming apparent resulting in adverse effects on computation. Increase in number of transistors also results in increased heat production which adversely affects computation. We have therefore hit a wall in terms of how many transistors we can squeeze onto a single chip.

| | COMPUTING ?

- While parallel computing looks good in principle, it in fact has it's own fair share of issues.
- Since the parallelism isn't inherent in the way it is being carried out, it must be artificially introduced by programming the computer to solve the task using the additional resources at hand; this isn't always easy to do.
- Moreover, not every problem can parallelized in this fashion.
- In quantum computing, the concept of parallelism is inherent.

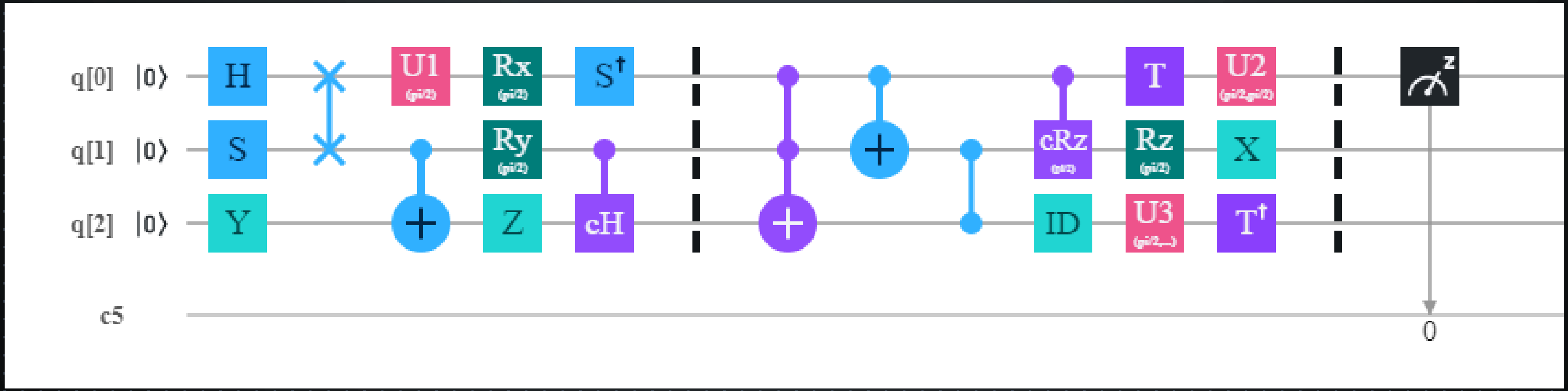
WHAT ABOUT REVERSIBLE CLASSICAL COMPUTING ?

- Landauer's principle is a physical principle which says that if the observer loses any information about a physical system, then the observer loses the ability to extract work from the system.

- In other words the more information about a system we lose, the more inefficient the system becomes.

- This is a serious consideration in the case of computation since , most of the operations we carry out are irreversible (think of a logical AND gate, given just the output bit, there is no way to determine the input bits).

- One solution is offered in the form of reversible computing, however, the number of extra bits introduce a large overhead.



II. WHAT IS QUANTUM COMPUTING ?

POWER OF QUANTUM COMPUTING

- QUANTUM SUPERPOSITION
- QUANTUM ENTANGLEMENT
- QUANTUM TUNNELING

Are you ready for this quantum ride ?

PLAY

WHAT IS A QUANTUM COMPUTER

A quantum computer is a machine that performs calculations based on the laws of quantum mechanics, which is the behavior of particles at the sub-atomic level. Its fundamental block unit is qubit.

QUBIT ? This sounds interesting !!!

- A bit of data is represented by a single atom that is in one of two states denoted by $|0\rangle$ and $|1\rangle$ (Bra-Ket notation) . A single bit of this form is known as a qubit.

- A physical implementation of a qubit could use the two energy levels of an atom. An excited state representing $|1\rangle$ and a ground state representing $|0\rangle$.

LET'S TOSS A , SHALL WE ?

- The simplest unit of information in classical systems, a bit, which can store either a 0 or a 1 value. When you toss a coin, the result will either be tails (1) or heads (0). This is a binary and deterministic state.

- For a quantum system, a qubit can be compared to a state where a coin is still spinning. Only upon measurement, do we get either heads $|0\rangle$ or tails $|1\rangle$.

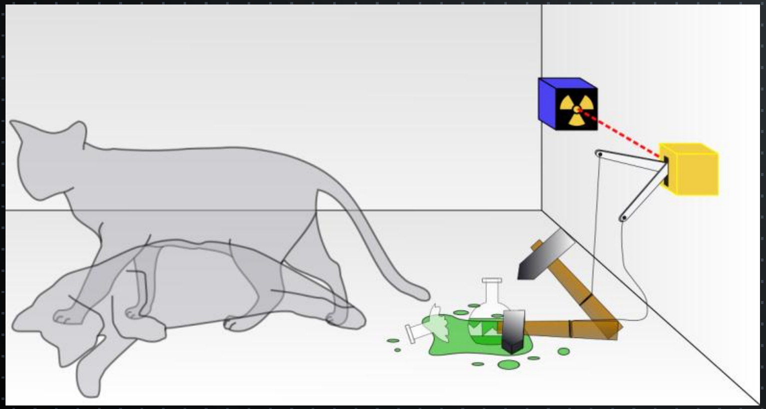
QUANTUM SUPERPOSITION

- A single qubit can be forced into a superposition of the two states denoted by the addition of the state vectors. Sometimes, when we have no evidence of the electron's state, we assume that it is in a superposition of both states such that

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

where α and β are complex numbers such that $\alpha^2 + \beta^2 = 1$ and α^2 represent the probability of the superposition collapsing to $|0\rangle$ and β^2 represent the probability of the superposition collapsing to $|1\rangle$. This defies the classical views of the world we live in and requires some mental effort fully grasp it!

THOUGHT EXPERIMENT



Schrodinger's Cat

A cat is placed in a steel box along with a Geiger counter, a vial of poison, a hammer, and a radioactive substance. When the radioactive substance decays, the Geiger detects it and triggers the hammer to release the poison, which subsequently kills the cat. The radioactive decay is a random process, and there is no way to predict when it will happen. The atom exists in superposition—both decayed and not decayed at the same time.

Until the box is opened, an observer doesn't know whether the cat is alive or dead—because the cat's fate is intrinsically tied to whether or not the atom has decayed and the cat would, as Schrödinger put it, be "living and dead ... in equal parts" until it is observed. This is the basis of **Copenhagen Interpretation**.

THE CENTURY OLD DEBATE

$$\Delta x \, . \, \Delta p \geq \frac{\hbar}{2}$$

Suppose you measure the position of a particle in motion and find it to be at point C. Where was the particle just before you make the measurement?

Note: Quantum Mechanics introduces indeterminacy i.e. you can only associate a probability with finding the particle at position C and can not find the position with determinacy.

QUANTUM SCHOOLS OF THOUGHT

Realist

The particle was at C. This seems like a sensible response which was also advocated by Einstein. If this is the case, then quantum mechanics (QM) is incomplete since, if the particle was at C and yet QM was unable to tell so due to indeterminacy. To a realist, indeterminacy is not a fact of nature, but a reflection of our ignorance. The position of the particle was never indeterminate, but merely unknown to the experimenter. There should be some hidden variables to the theory of QM.

Orthodox

The particle wasn't really anywhere. It was the act of measurement that forced the particle to take a stand. Though how and why it decided on the point C, we dare not ask. Observations not only disturb what is to be measured, they produce it. We compel the particle to assume a definite position. This view is the Copenhagen Interpretation. This is the most widely accepted position. But, it introduces peculiarities about the act of measurement.

Agnostic

Refuse to answer. This is not quite as silly as it sounds. What sense can there be in making assertions about the status of a particle before a measurement, when the only way of knowing whether you were right is precisely to conduct a measurement, in which case, what you get is no longer "before the measurement". It is metaphysics. Experiments have confirmed the Copenhagen Interpretation.

QUANTUM MEASUREMENT

Suppose you make a second measurement, immediately after the first?
Would you get C again, or does the act of measurement cough up some completely new number?

On this question, everyone is in agreement. A repeated measurement for the same particle must return the same value. Indeed, it would be tough to prove that the particle was really found at C, in the first instance, if this could not be confirmed by immediate repetition of the measurement. The first measurement radically alters the state of the system to point at C. This is known as collapse (that we earlier talked about) and the second measurement must be made quickly to again give the value C, otherwise the state of the system can change.

- Consider a 3 bit qubit register. An equally weighted superposition of all possible states would be denoted by:

$$|\psi\rangle = \underbrace{\frac{1}{\sqrt{8}}|000\rangle}_{0} + \underbrace{\frac{1}{\sqrt{8}}|001\rangle}_{1} + \underbrace{\frac{1}{\sqrt{8}}|010\rangle}_{2} + \underbrace{\frac{1}{\sqrt{8}}|011\rangle}_{3} + \underbrace{\frac{1}{\sqrt{8}}|100\rangle}_{4} + \underbrace{\frac{1}{\sqrt{8}}|101\rangle}_{5} + \underbrace{\frac{1}{\sqrt{8}}|110\rangle}_{6} + \underbrace{\frac{1}{\sqrt{8}}|111\rangle}_{7}$$

- In general, an n qubit register can represent the numbers 0 through $2^n - 1$ simultaneously.

- If we attempt to retrieve the values by measurement represented within a superposition, the superposition randomly collapses to represent just one of the original values.

- But what is this state $|000\rangle$? All three qubits in the register are in state $|0\rangle$.

QUANTUM ENTANGLEMENT ?

- ❖ Entanglement is the ability of quantum systems to exhibit correlations between states within a superposition.
- ❖ Imagine two qubits, each in the state $\alpha|0\rangle + \beta|1\rangle$. We can entangle the two qubits such that the measurement of one qubit is always correlated to the measurement of the other qubit.
- ❖ Spooky action at a distance: When it came to the idea that two particles can be entangled, and an effect on one could be instantaneously felt by the other even over vast distances, for Einstein that was simply unbelievable. He dubbed it "spooky action at a distance".
- ❖ When particles are entangled. their properties or states, like spin, will be linked. But until they are measured, those properties will remain in superposition, meaning it can be in multiple states at once. Observing one particle will make it take on one state, while at the same exact moment, it's entangled twin will take on the opposite state (so as to conserve the total angular momentum).

III. THE MAGIC

QUANTUM GATES

- Due to the nature of quantum physics and Landauer's Principle, the destruction of information in a gate will cause heat to be emitted which can destroy the superposition of qubits. Thus, the classical gates cannot be used. We must use *quantum gates*.
- Quantum Gates are similar to classical gates, but do not have a degenerate output. i.e. their original input state can be derived from their output state, uniquely. They must be reversible.
- This means that a deterministic computation can be performed on a quantum computer only if it is reversible. Luckily, it has been shown by Charles Bennet in 1973 that any deterministic computation can be made reversible.

PAULI Z

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

PAULI X

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

PAULI Y

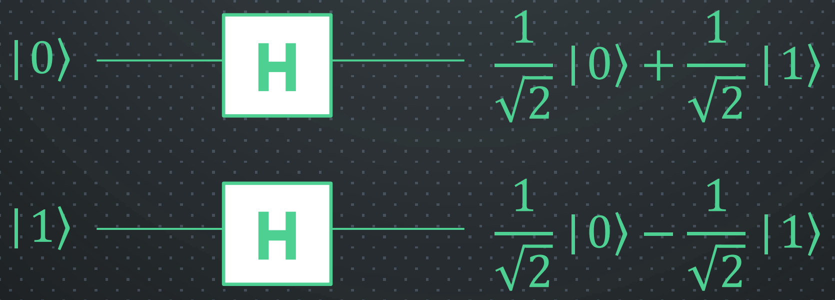
$$\begin{pmatrix} 0 & -\imath \\ \imath & 0 \end{pmatrix}$$

LET'S PLAY WITH SIMPLE QUANTUM GATES

NOT GATE

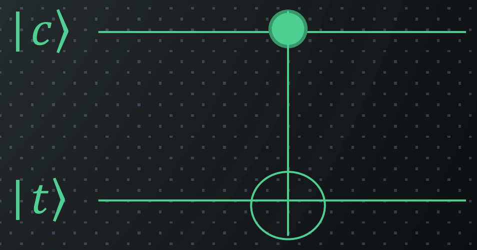
NOT gate inverts the state.

HADAMARD GATE



Hadamard gate creates an equal superposition.

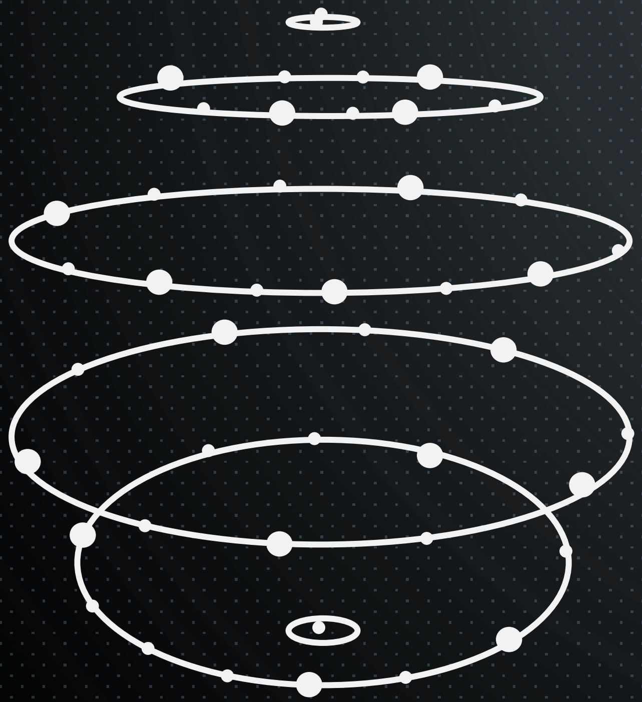
CNOT GATE



INPUT $|c\rangle$	INPUT $|t\rangle$	OUTPUT $|c\rangle$	OUTPUT $|t\rangle$
$|0\rangle$	$|0\rangle$	$|0\rangle$	$|0\rangle$
$|0\rangle$	$|1\rangle$	$|0\rangle$	$|1\rangle$
$|1\rangle$	$|0\rangle$	$|1\rangle$	$|1\rangle$
$|1\rangle$	$|1\rangle$	$|1\rangle$	$|0\rangle$

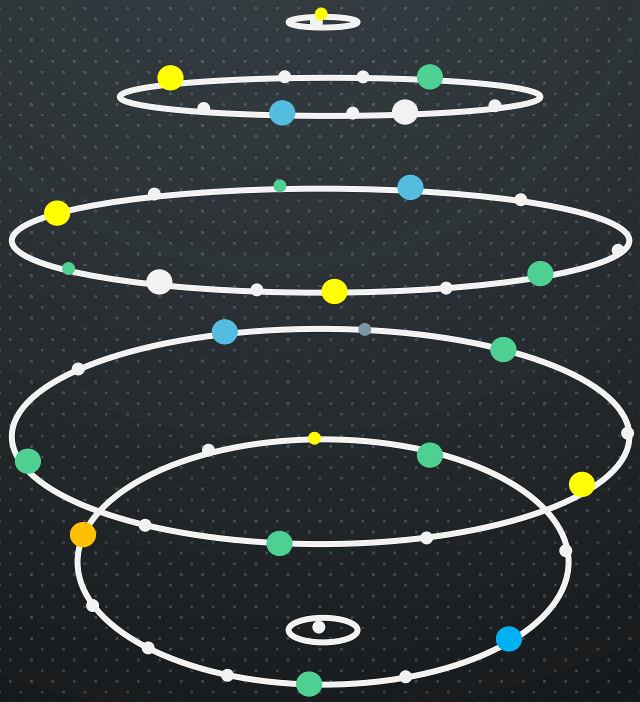
CNOT gate is a two-qubit entangling gate which flips the target qubit if the control qubit is $|1\rangle$

HOW DO QUANTUM ALGORITHMS WORK ?



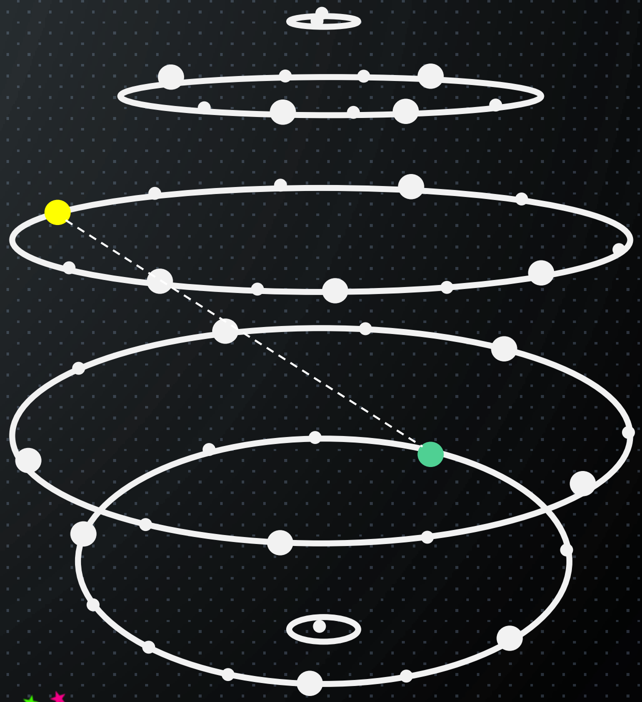
Superposition

Create a superposition of 2^n states using quantum gates that you have just learned.



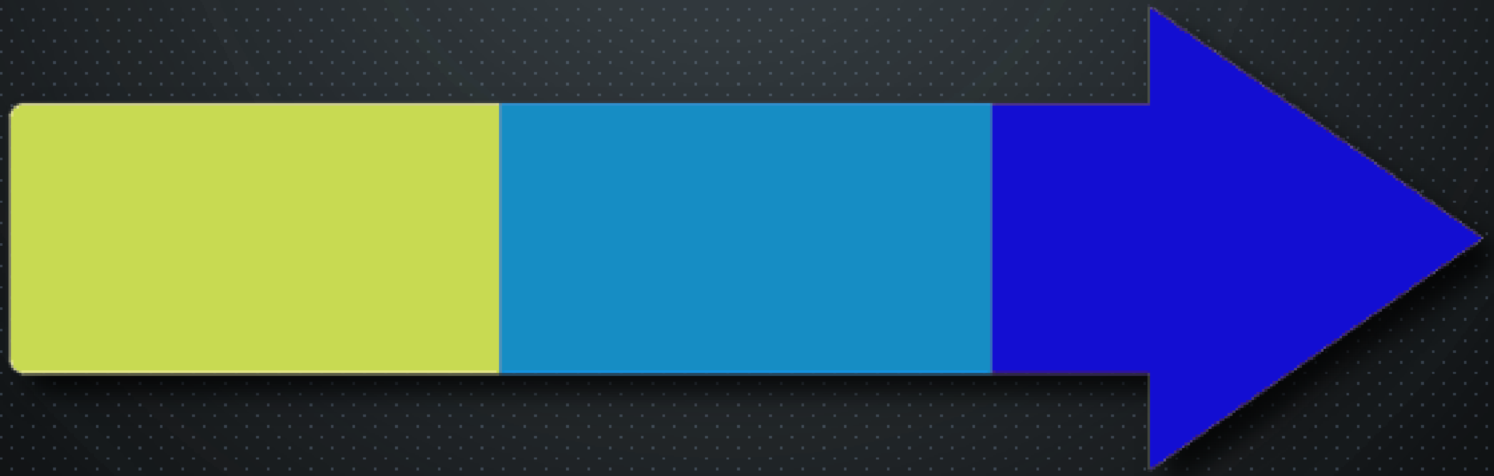
Encoding The Problem

Encode your problem by putting phases on all 2^n states



Quantum Magic

QC interferes these states back to a few outcomes containing the solution



IV. QUANTUM COMPUTING TIMELINE

A Brief History of Quantum Computing

1982

Feynman proposed the idea of creating computing machines based on the laws of quantum mechanics.

1985

David Deutsch developed the Quantum Turing Machine, showing that quantum circuits are universal.

1994

Peter Shor came up with a quantum algorithm to factor very large numbers in polynomial time.

1997

Lov Grover developed a quantum search algorithm with $O(\sqrt{n})$ complexity which classically is $O(n)$.

2001

15=3x5

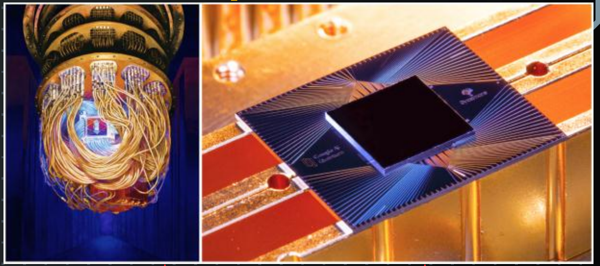
BYE RSA !!!

A 7 qubit machine was built and programmed to run Shor's algorithm to successfully factor 15.

A New! Era of Quantum Computing

Laflamme is a PhD student of Stephen Hawking

Sycamore



2002

IQC

Institute for Quantum Computing was established at Waterloo University by Mosca, Laflamme and Laziridis.

2003

Balanced Vs. Constant

Implementation of the “Deutsch-Jozsa Algorithm” was achieved on an ion trap computer at University of Innsbruck

2009

Solve Ax = b

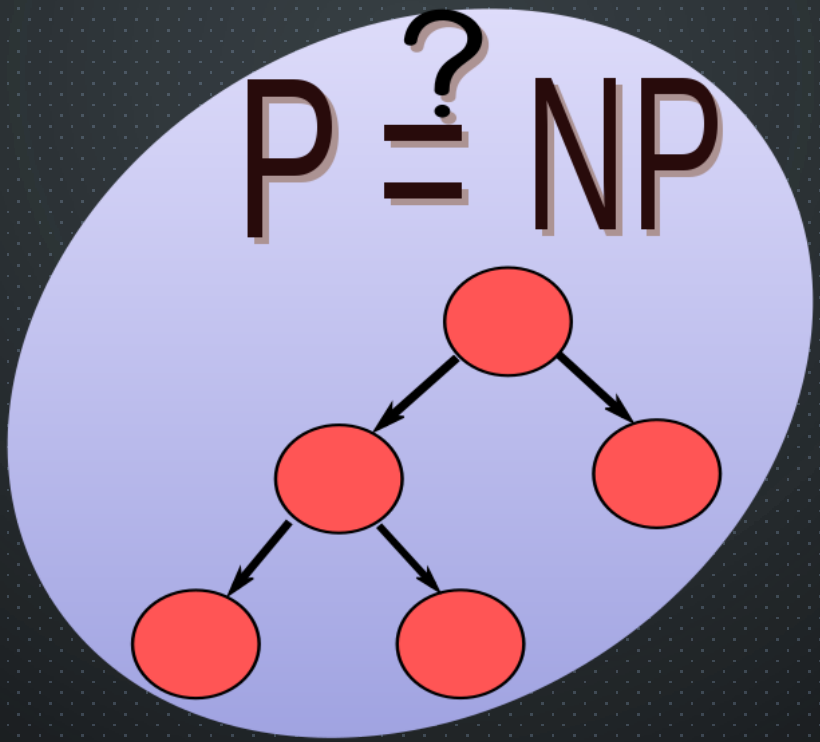
Harrow, Hasidim and Lloyd gave a computational speedup $O\left((\log N)k^2\right)$ for Ax = b over its classical counterpart $O(Nk)$.

2013

First Hybrid Algorithm: Variational Quantum Eigensolver (VQE) Algorithm found the ground state energy of H-He+

2019

Google Quantum Supremacy Experiment: Sampled random instances of a 53-qubit quantum circuit in 200 seconds.



V. APPLICATIONS IN CS

QC SUCCESS STORIES OVER CC

Constant or Balanced Function: Suppose, we are given a black box known as oracle that implements some function $f: \{0,1\}^n \rightarrow \{0,1\}$. The function takes n-digit binary values as input and produces either a 0 or a 1 as output for each such value. We are promised that the function is either constant (0 on all outputs or 1 on all outputs) or *balanced* (returns 1 for half of the input domain and 0 for the other half). The task is to determine whether f is constant or balanced.

Classical Complexity	Quantum Complexity (Deutsch - Jozsa Algorithm)
$\boldsymbol{O}(\mathbf{2}^{\boldsymbol{n}})$	$\boldsymbol{O}(\mathbf{1})$

Database Search: What is the time and space complexity to search an unsorted database with N entries?

	Classical Complexity	Quantum Complexity (Grover Algorithm)
Time	$\boldsymbol{O}(\boldsymbol{n})$	$\boldsymbol{O}(\sqrt{\boldsymbol{n}})$
Storage Space	$\boldsymbol{O}(\boldsymbol{n})$	$\boldsymbol{O}(\log \boldsymbol{n})$

JUST WOW !!!

Find period: Assume that we are given an n-bit input k-bit output Boolean function f. Say, we are also given a promise that the function f is such that for any two n-bit inputs x and y, f(x) = f(y) if and only if $x = y \oplus s$ for some $s \in \{0,1\}^n$. Is it possible to determine the shift s?

Classical Complexity	Quantum Complexity (Simon Algorithm)
$O(2^n)$	$O(n)$

Factorize: Given a composite integer N=p*q, find its factors.

Classical Complexity	Quantum Complexity (Shor Algorithm)
$O\left(e^{1.9(\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}}}\right)$	$O\left((\log N)^2(\log\log N)(\log\log\log N)\right)$

LINEAR SYSTEM OF EQUATIONS Ax=b

- **Find x:** Given N equations represented in the matrix form Ax=b. We are interested in the result of a scalar measurement M on the solution vector x, instead of the values of the solution vector itself.

Let's first look into some terms before discussing the complexity.

- Sparsity s: Ratio of the number of zero elements to the number of non-zero elements in the matrix
- Precision ϵ: Precision to the solution x
- Condition Number k: Ratio of maximum and minimum singular values of a matrix

Classical Complexity (Conjugate Gradient Descent Method)	Quantum Complexity (Harrow Hassidim Lloyd (HHL) Algorithm)
$O\left(Nsk\left(\log\frac{1}{\epsilon}\right)\right)$	$O\left(\frac{(\log N)s^2k^2}{\epsilon}\right)$

$$O\left(\frac{\sqrt{N}polylog(N)k^2}{\epsilon}\right)$$

WOSSNIG (2017)

Reduce dependence on s, for dense matrices

Improvements over HHL (2009)

$$O\left(\frac{(\log N)s^2k^2}{\epsilon}\right)$$

Reduce dependence on k

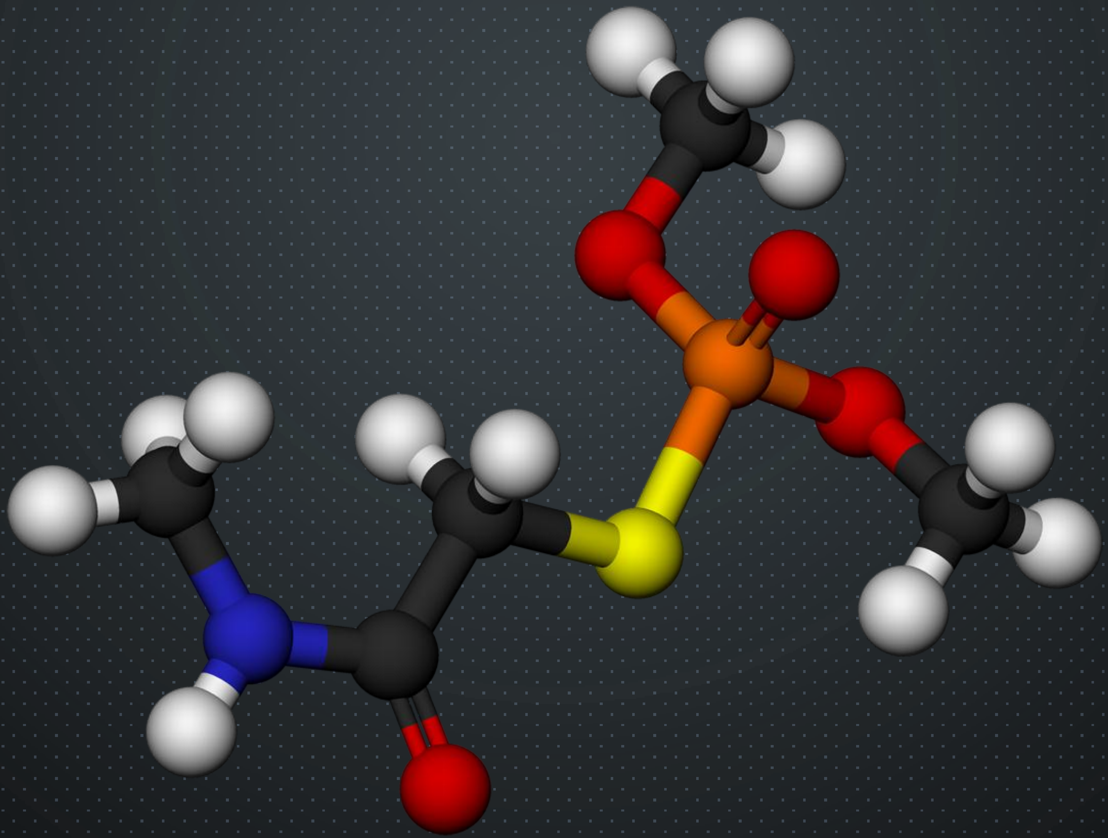
Reduce dependence on ϵ

$$O\left(\frac{(\log N)s^2k(\log k)^3}{\epsilon}\right)$$

AMBIANIS (2010)

$$O\left(\log N\, s^2k^2\left(\log\frac{1}{\epsilon}\right)\right)$$

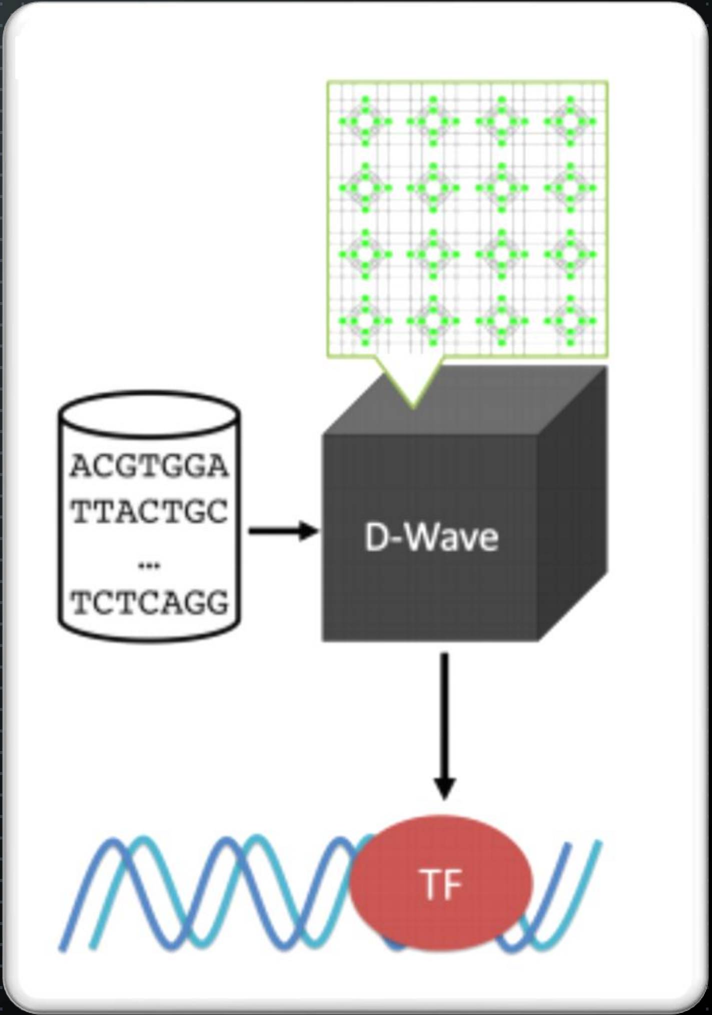
CHILDS (2018)



VI. APPLICATIONS IN BIOCHEMISTRY

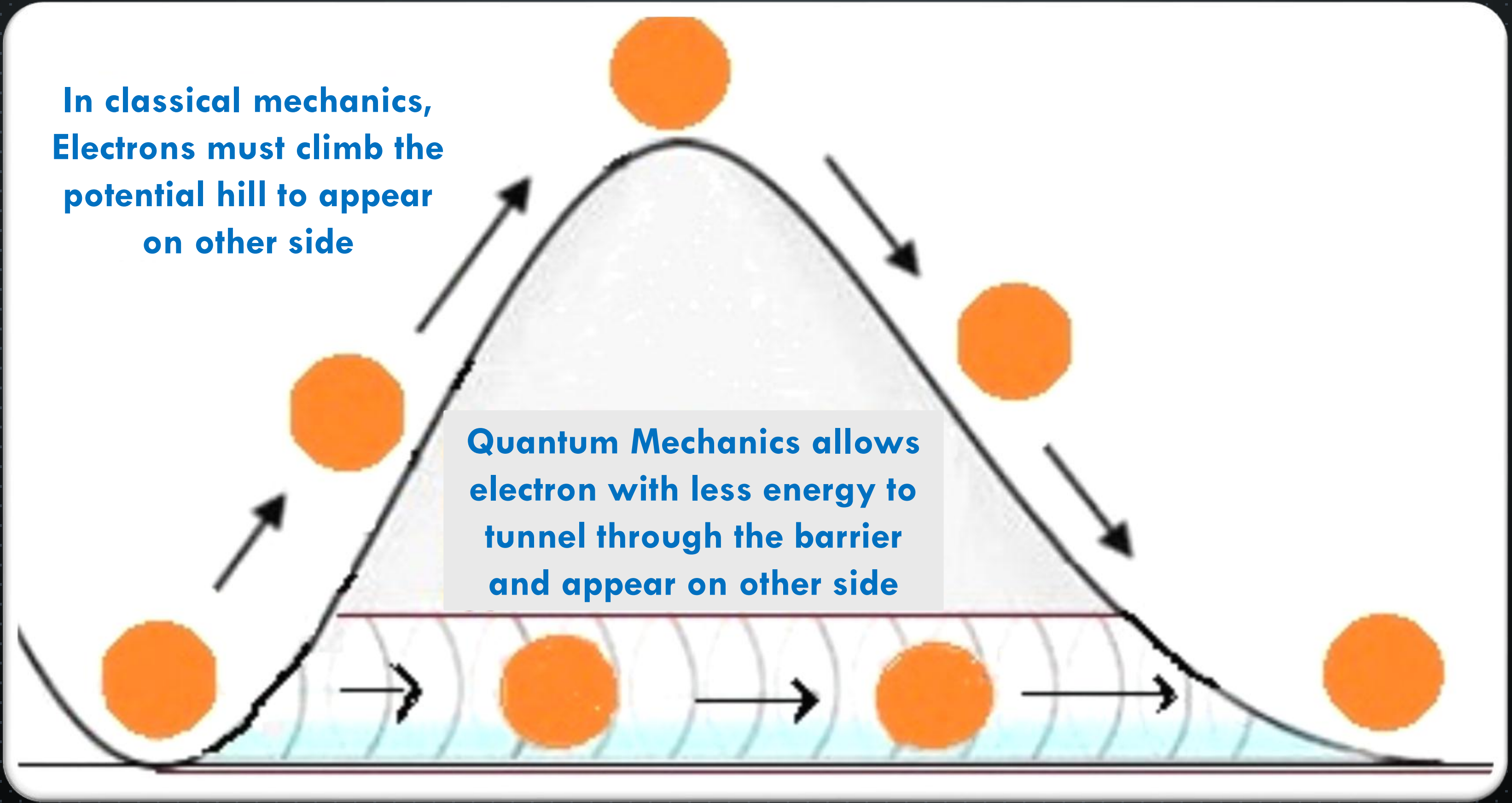
HOW TO CLASSIFY AND RANK TRANSCRIPTION FACTOR-DNA BINDING EVENTS

- **Problem statement**: Gene expression is regulated and controlled by transcription factors (TF). It is still a bone of contention how they specifically bind to their DNA targets. Many machine models are used to extract this information, classify and rank these binding affinities. To model this problem, the binding preference for a TF of a DNA sequence of length L is represented as a 4 x L matrix corresponding to all the 4 DNA alphabets {A,C,T,G}. Each matrix element is indicative of the contribution of the nucleotide at that particular location to the total binding affinity. Then, a machine learning algorithm is implemented on a D-WAVE system (quantum annealer).



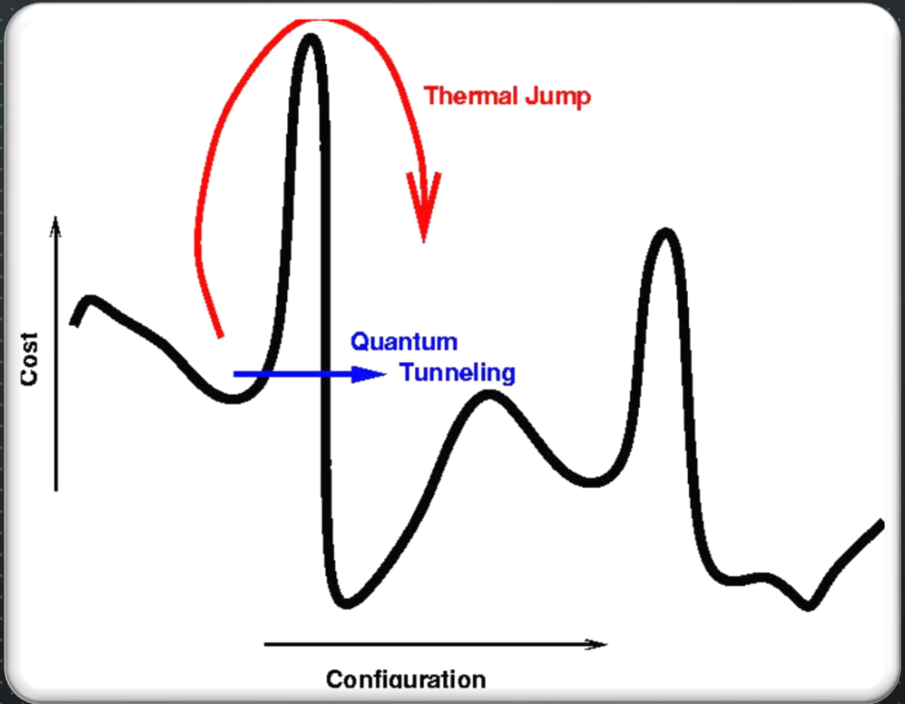
We are now going to understand how a quantum annealer works

LET'S TUNNEL



Quantum tunneling is projected to create physical limits to the size of the transistors used in microprocessors, due to electrons being able to *tunnel* past them if the transistors are too small which will produce wrong results. **This is a major problem that we talked at the very beginning with the classical computers.**

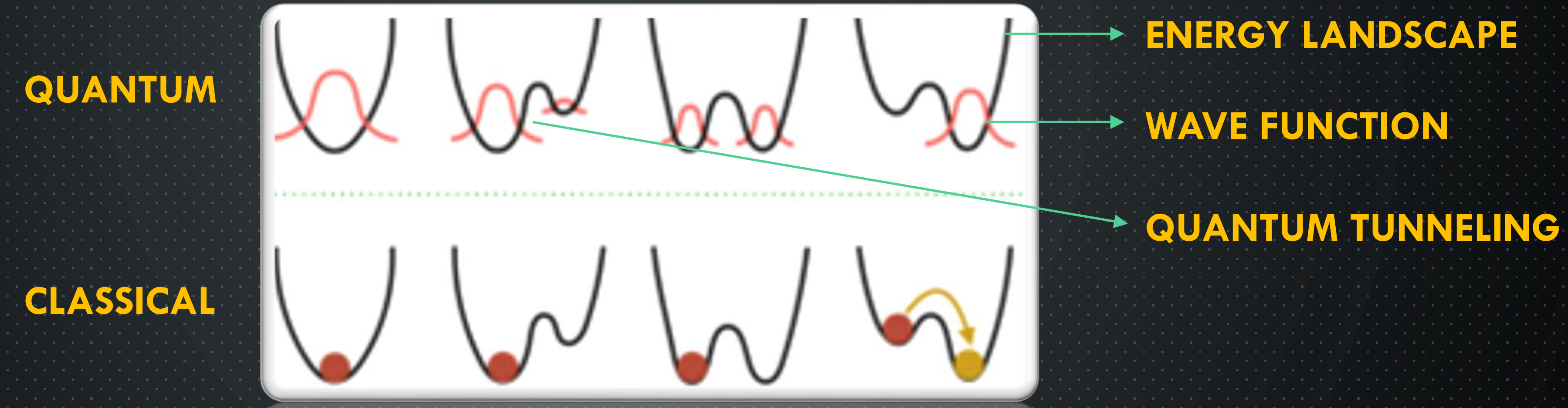
QUANTUM ANNEALING



- Quantum annealing is similar to classical or simulated annealing, where thermal fluctuations allow the system to jump between different local minima in the energy landscape. As the temperature is lowered, the probability of moving to a worse solution tends to zero.

- In quantum annealing, these jumps are driven by quantum tunneling events as discussed in last slide. This process explores the landscape of local minima more efficiently than thermal noise, especially when the energy barriers are tall and narrow.

SOLVING USING QUANTUM ANNEALING



The adiabatic theorem in quantum mechanics states that a system remains in its ground state provided the external perturbation acts very slowly and if there remains a sufficient gap between the ground state and the rest of the energy spectrum during the application of the perturbation. We use adiabatic quantum computation in which we encode our cost function into the ground state of the problem Hamiltonian H_p with certain penalties. The aim is then to find the minimum value of this Hamiltonian. We prepare our system into the ground state of a Hamiltonian H_0 whose ground state energy is known and that it can be easily prepared. We then interpolate from H_0 to H_p at the end of the annealing time or the time of the evolution (T) such that

$$H = \left(1 - \frac{t}{T}\right) H_0 + \left(\frac{t}{T}\right) H_p$$

At t=0, we are in state with total Hamiltonian H_0 and at the end of the annealing time, we land in our problem system Hamiltonian H_p. During the course of the perturbation, even though the wave function keeps changing, but we land ourselves finally in the ground state wave function of our problem Hamiltonian.

MACHINE LEARNING ON QUANTUM ANNEALER

Given: N experimental data sets i.e. N sequences of length L and fluorescence intensity as a measure of the binding affinity. Nth sequence is represented by $x_n = \left(x_{n,1}, \dots\dots\dots, x_{n,L}\right)$ with $x_{n,i} \epsilon \{A, C, T, G\}$, for i=1,….., L
A one-shot encoding to represent the sequence as a vector of binary variables: A = 1000, C = 0100, G = 0010, T = 0001 to give a feature vector $\vec{\varphi_n}$

Minimize: $H_{classical} = \sum_{n=1}^{N} (y_n - \vec{w}^T \vec{\varphi_n})^2 + \lambda ||w||_1$

Parameter Definition: $\vec{w} = (w_1, \dots\dots\dots, w_{4L})$ are binary weights, $||w||_1 = \sum_{m=1}^{4L} w_m$ is the number of non-zero terms, λ is the regularization term added to avoid overfitting, $\vec{\varphi_n} = \left(\varphi_{n,1}, \dots\dots\dots, \varphi_{n,4L}\right)^T$ is the transformed feature vector and y_n is the binding affinity.

Classical Problem Hamiltonian:

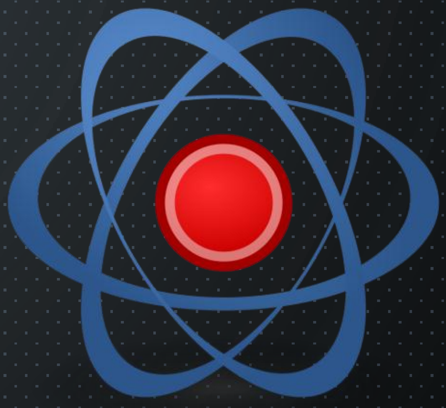
$$H_p = \arg\min_{w} \vec{w}^T \left(\sum_n \vec{\varphi_n} \vec{\varphi_n}^T\right) w + \vec{w}^T \left(\lambda \mathbb{I} - 2 \sum_n y_n \vec{\varphi_n}\right)$$

PERFORMANCE

- D-Wave system performed comparably or slightly better than classical counterparts for classification when the training size is small, and competitively for ranking tasks.

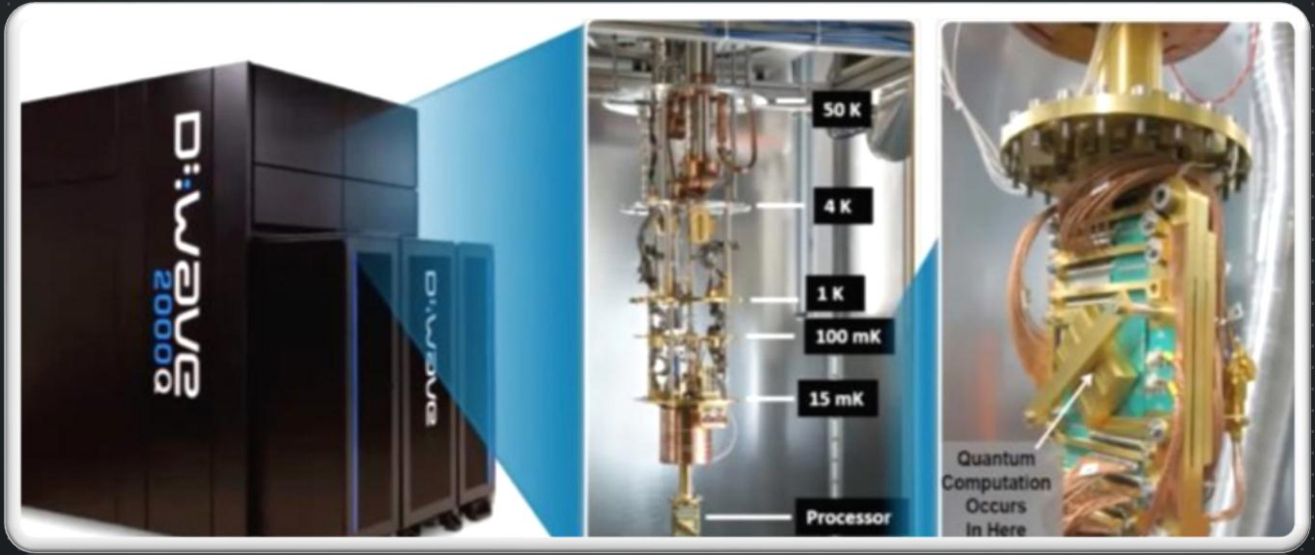
- It has been demonstrated that the feature weights obtained by DW reflect biological knowledge.

- This gives some confidence that quantum annealing (QA) is learning relevant biological patterns from the data.



VII. APPLICATIONS IN OTHER DOMAINS

FINANCE



- **Dynamic Portfolio Optimization**: Given a selection of assets i, with $i \in [1, n]$, the goal is to maximize the final profits at time $t = T$. Let $x_{i,t}$ be the amount of money we choose invest in asset i at time $t \in [0, T-1]$, and let $R_{i,t+1}$ be the returns resulting from this decision. Given a return $R_{i,t+1}$, the decision to invest $x_{i,t+1}$ at the next time step is usually computed iteratively.

- **Implementation:** This problem was solved on two **D-Wave chips (quantum annealers)** with 512 and 1152 qubits. While only small instances were implemented, the performance of the quantum annealers was similar to that of classical hardware. These experiments proved that this problem can be solved on the D-Wave machine with a high success rate. It was also observed that a proper fine-tuning of the D-Wave machines allowed for important improvements in success rates.

CHEMISTRY

- **Spin Quantum Numbers (s)**: In chemistry, it is very imperative to determine the spin quantum numbers of an arbitrary function. Sugisaki et. al. gave a novel quantum algorithm to determine whether quantum chemical calculations performed on quantum computers give correct wave functions as exact solutions of Schrodinger equation in a desired manner. They have proposed a quantum circuit to simulate the time evolution of wave functions under an S^2 operator and integrated it into the quantum phase estimation (QPE) circuit enabling us to determine the spin quantum number of the arbitrary wave functions. They demonstrated that the spin quantum numbers of up to three spins can be determined by only one qubit measurement in QPE.

$$S^2|\psi(S)\rangle = s(s+1)\,|\psi(S)\rangle$$

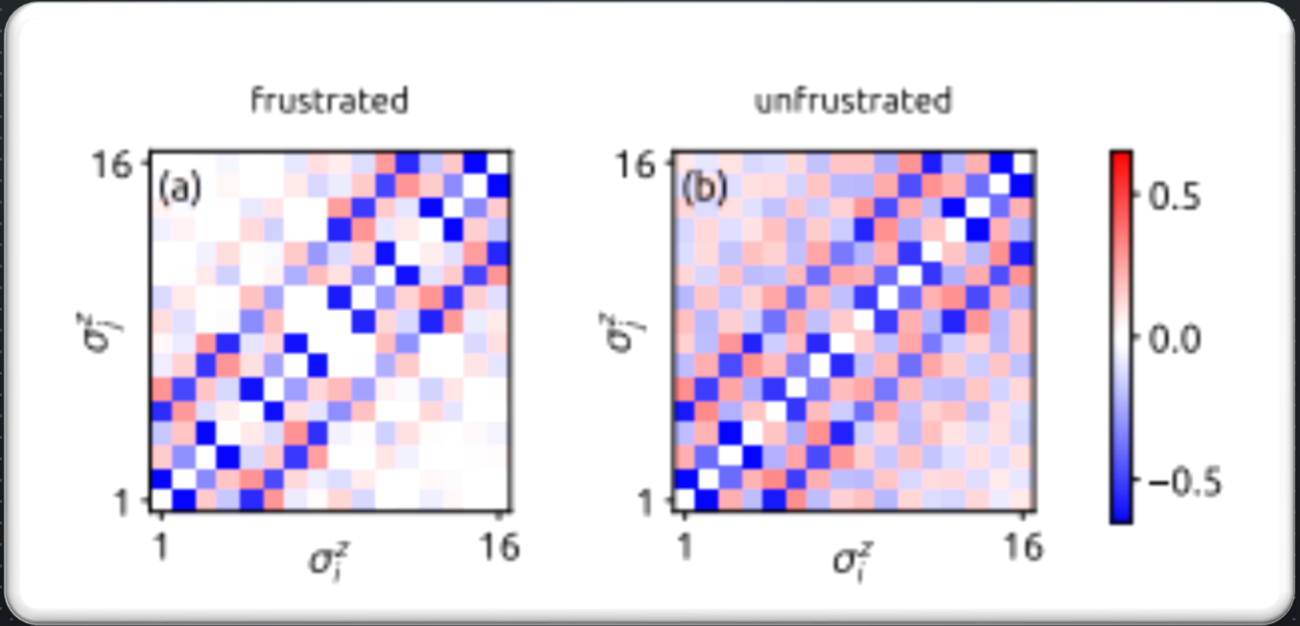
Operator   Wave-function   Spin number (Find this value)

$$e^{-\iota S^2 t}|\psi(S)\rangle = e^{-\iota s(s+1)t}|\psi(S)\rangle = e^{-2\pi\iota\varphi}|\psi(S)\rangle$$

Using QPE, one can find s in terms of phase φ

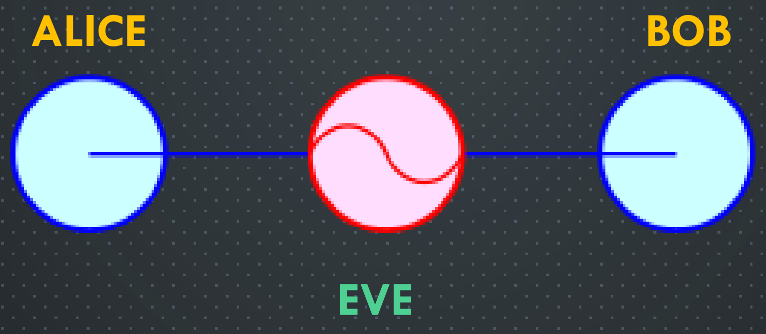
Sugisaki, Kenji & Nakazawa, Shigeaki & Toyota, Kazuo & Sato, Kazunobu & Shiomi, Daisuke & Takui, Takeji. (2019). Quantum chemistry on quantum computers: quantum simulations of the time evolution of wave functions under the S 2 operator and determination of the spin quantum number S. Physical Chemistry Chemical Physics. 10.1039/C9CP02546D.

PHYSICS



- **Frustrated Heisenberg Model** : Find the lowest energy eigenvalue of a frustrated Heisenberg model on a given lattice. We make use of Variational Quantum Eigensolver (VQE) in which we prepare a parametrized quantum circuit which upon measurement gives the eigenvector with the lowest energy eigenvalue. The parameters are optimized over a classical computer and fed back to the quantum computer. This is done until convergence to find the minimum ground state energy. We map our objective function to a quantum Hamiltonian. This is a hybrid algorithm, very suitable and efficient in the future due to reasons which I shall cover in the upcoming slides.

QUANTUM CRYPTOGRAPHY



- The best known application of quantum cryptography is in quantum key distribution which offers an information-theoretically secure solution to the key exchange problem.

- The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e. non-quantum) communication.

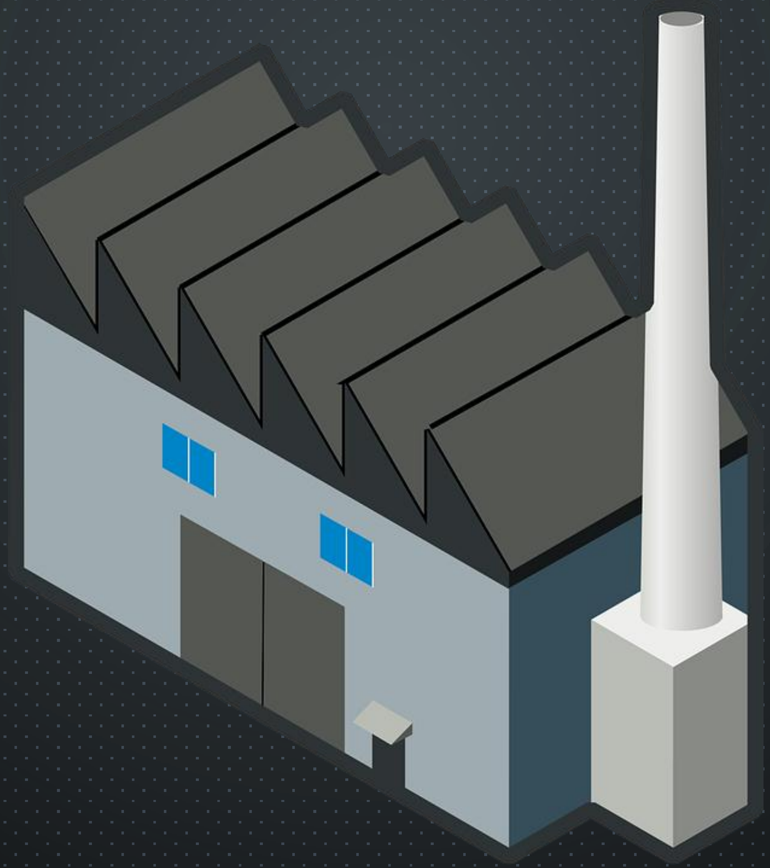
- For example, it is impossible to copy data encoded in a quantum state. If one attempts to read the encoded data, the quantum state will be changed (no-cloning theorem). This could be used to detect eavesdropping in quantum key distribution.

QC- A BREAKTHROUGH IN ALL DOMAINS

- **Artificial Intelligence:** A primary application for quantum computing is artificial intelligence (AI). AI is based on the principle of learning from experience, becoming more accurate as feedback is given, until the computer program appears to exhibit “intelligence.” This feedback is based on calculating the probabilities for many possible choices, and so AI is an ideal candidate for quantum computation. It promises to disrupt every industry, from automotive to medicine. Google is using a quantum computer to design software that can distinguish cars from landmarks.

- **Molecular Modelling:** Chemical reactions are quantum in nature as they form highly entangled quantum superposition states. But fully-developed quantum computers would not have any difficulty evaluating even the most complex processes. Google has already made forays in this field by simulating the energy of hydrogen molecules.

- **Weather Forecasting:** Seth Lloyd and colleagues at MIT have shown that the equations governing the weather possess a hidden wave nature which are amenable to solution by a quantum computer. Director of engineering at Google, Hartmut Neven also noted that quantum computers could help build better climate models that could give us more insight into how humans are influencing the environment.



VIII. INDUSTRY COMPETITORS

QUANTUM RACE IS ON!

IBM

- Developed a 50 qubit quantum computer by 2017 end. You can now access a 14-qubit IBMQ processor. IBM's recently unveiled IBM Q System One quantum computer (which can be rented), with a fourth-generation 20-qubit processor, has produced a Quantum Volume of 16, roughly double that of the current IBM Q 20-qubit IBM Q Network devices, which have a Quantum Volume of 8.

- IBM reveals its biggest yet quantum computer, consisting of 53 qubits in 2019.

GOOGLE

- Google announced the creation of a 72-qubit quantum chip in 2018,
- called "Bristlecone", achieving a new record.

- Quantum Supremacy Breakthrough 2019: Google claimed that its 54-qubit (one faulty qubit) Sycamore processor was able to perform a calculation in 200 seconds that would have taken the world's most powerful supercomputer 10,000 years. IBM claims that same task could be performed on a classical system in just 2.5 days. Google's quantum supremacy can potentially mark the end of the bitcoin in 2020.

WHO WILL WIN ?

MICROSOFT

Microsoft

- Claims to have built a topological quantum computer.
- They claim that their new system will allow users to control up to 50,000 qubits using three wires. Microsoft has also developed a new cryogenic CMOS design and a 1- cm^2 chip for computing at near absolute zero temperatures.
- Programs in Q# can be executed locally on a 32-qubit simulator, or a 40-qubit simulator on Azure.

D-WAVE SYSTEMS

D:WAVE
The Quantum Computing Company™

- D-Wave Systems: Sells 2000-qubit processors suited for optimization problems using quantum annealing.
- There is a lot of skepticism on their performance.

NOBODY WANTS TO LOSE !!!

IONQ

- On December 17, 2018, the company IonQ based at College Park, Maryland introduced the first commercial trapped-ion quantum computer, with a program length of over 60 two-qubit gates, 11 fully connected qubits, 55 addressable pairs, one-qubit gate error <0.03% and two-qubit gate error <1.0%

- IonQ claims that trapped ions could provide a number of benefits over other physical qubit types in accuracy, scalability, predictability, and coherence time.

RIGETTI

- By Spring of 2017, the company based in Berkeley was testing eight-qubit superconducting quantum computers, and in June, the company announced the public beta availability of a quantum cloud computing platform called Forest 1.0, which allows developers to write quantum algorithms for a simulation of a quantum chip with 36 qubits.

- Preparing to launch a 128-qubit chip in 2020.

IONQ IBM

IBM RIGETTI

ERA OF QUANTUM COLD WAR ?

USA

- **Penetrating Hard Targets (PHT): This project came into news from the NSA leak by Edward Snowden and the purpose is to build a Quantum Computer capable of breaking current encryption mechanisms. The current progress is unknown.**
- **On December 21, 2018, the National Quantum Initiative Act was signed into law by President Donald Trump, establishing the goals and priorities for a 10-year plan to accelerate the development of quantum information science and technology applications in the United States.**

CHINA

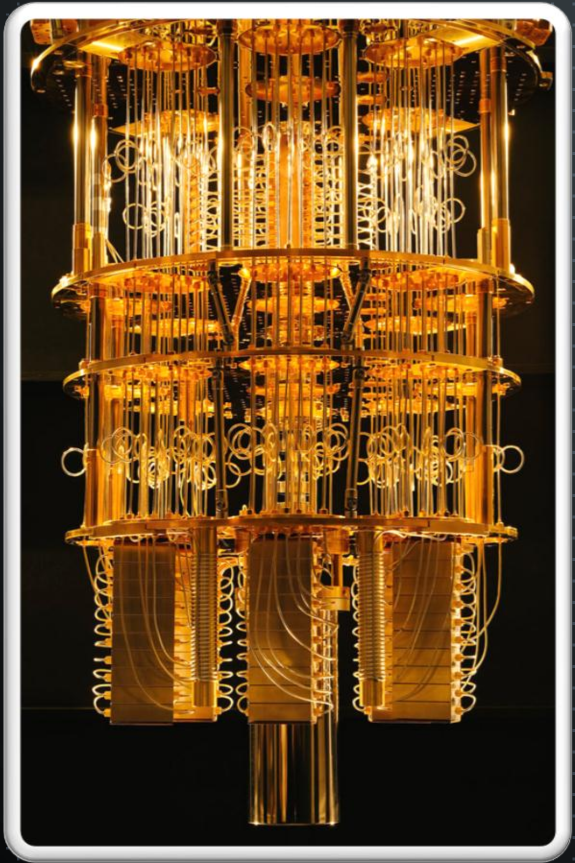
- **The latest reported record distance for quantum teleportation is 1,400 km (870 mi) by the group of Jian-Wei Pan using the Micius satellite for space-based quantum teleportation. With Micius, Chinese researchers are attempting to use photonic quantum technology to develop new forms of secure communications that would be unbreakable.**
- **It is reportedly investing $10bn in building the National Laboratory for Quantum Information Sciences in Hefei.**



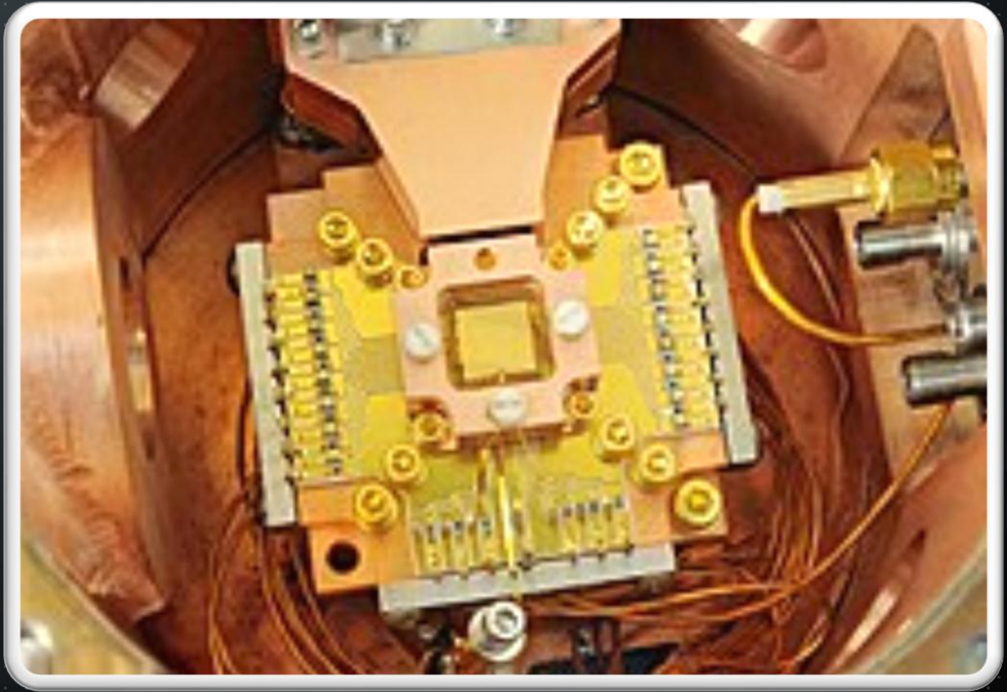


IX. WHAT LIES AHEAD ?

QC HARDWARE



SUPERCONDUCTING QC



ION TRAP QC

Problem WITH QUBITS

- Quantum computers are exceedingly difficult to engineer, build and program. As a result, they are crippled by errors in the form of noise, faults and loss of quantum coherence, which is crucial to their operation and yet falls apart before any nontrivial program has a chance to run to completion.

- This loss of coherence (called decoherence), caused by vibrations, temperature fluctuations, electromagnetic waves and other interactions with the outside environment, ultimately destroys the exotic quantum properties of the computer.

- Given the current pervasiveness of decoherence and other errors, contemporary quantum computers might be unlikely to return correct answers for programs of even modest execution time.

THE BILLION DOLLAR QUESTION

How do we get useful results out of a quantum computer that becomes unusably unreliable before completing a typical computation?

Look for hybrid algorithms that make use of both classical and quantum computers.

YAY !!

“When you change the way you look at things, the things you look at change”

- Max Planck

(Father of Quantum Mechanics)

ANY QUESTIONS