QUANTUM COMPUTING

Presentation in Physics

CONTENTS


INTRODUCTION AND BRIEF HISTORY
71. Pranav Walvekar


NEED FOR QUANTUM COMPUTERS
49. Varad Talegaonkar


ANALOGIES
76. Parth Zarekar


CONCEPTS AND PHYSICAL MANIFESTATION
54. Krishnaraj


APPLICATIONS ON WEATHER FORECASTINGAND FINANCIAL MODELLING
50. Atharva Tanawade


44. Devanshu Surana
APPLICATIONS ON CRYPTOGRAPHY, DRUGS AND AI AND ML

INTRODUCTION AND BRIEF HISTORY

71. Pranav Walvekar

WHAT IS QUANTUM COMPUTING

Quantum computing is a type of computation that harnesses the collective properties of quantum states, such as superposition, interference, and entanglement, to perform calculations.

The devices that perform quantum computations are known as quantum computers Though current quantum computers are too small to outperform usual (classical) computers for practical applications, they are believed to be capable of solving certain computational problems, such as integer factorization (which underlies RSA encryption), substantially faster than classical computers.

BIRTH OF QUANTUM COMPUTING

Quantum computing began in 1980 when physicist Paul Benioff proposed a quantum mechanical model of the Turing machine. Richard Feynman and Yuri Manin later suggested that a quantum computer had the potential to simulate things a classical computer could not feasibly do.

NEED FOR QUANTUM COMPUTERS

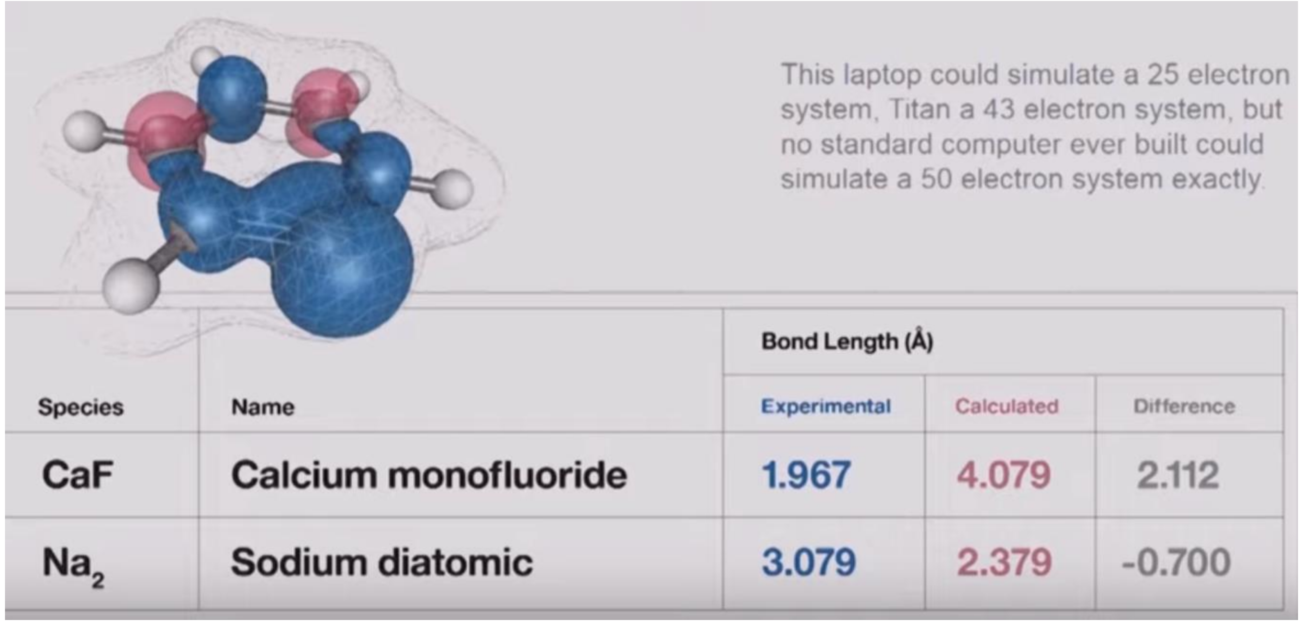
49. Varad Talegaonkar

Why do we need quantum computers

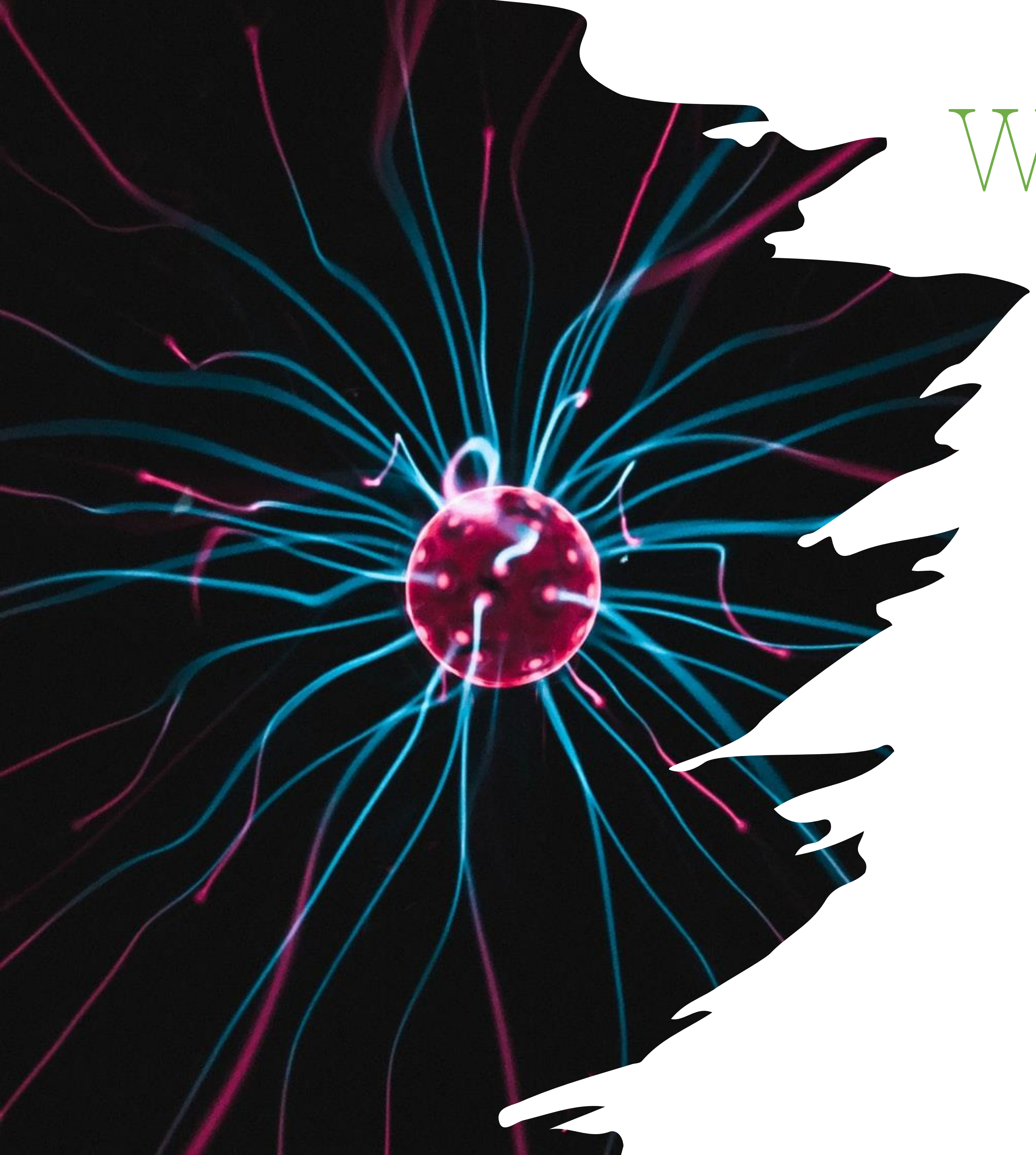
The most fundamental question giving rise to the idea of quantum computing was "Can we simulate physics on a computer?".

With this, even scientists and engineers started to notice limitations in the classical computers to solve very complex problems. Hence a need for quantum computing was felt.

Richard Feynman took one step further and proposed If we cannot simulate quantum physics on a classical computer, maybe we can build a quantum mechanical computer which would be better than the classical computers



Species	Name	Bond Length (Å)		
		Experimental	Calculated	Difference
CaF	Calcium monofluoride	1.967	4.079	2.112
Na_2	Sodium diatomic	3.079	2.379	-0.700



WHAT IS A QUBIT

- A qubit (or quantum bit) is the quantum mechanical analogue of a classical bit.
- A qubit is a two-level quantum system having $|0\rangle$ and $|1\rangle$ as two basis quantum states.
- Multiple implementations of a qubit are discussed, few examples are -
- polarizations of a photon, two of the (multiple) discrete energy levels of an ion, a superconducting Transmon qubit, the nuclear spin states of an atom or the spin states of an electron.

- The amount of information a qubit system can represent grows exponentially. Information that 500 qubits can easily represent would not be possible with even more than 2^500 classical bits.
- It would take a classical computer millions of years to find the prime factors of a 2,048-bit number. Qubits could perform the calculation in just minutes.

QUANTUM COMPUTING

Current quantum programming languages and compilers are mainly focused on optimizing low-level circuits consisting of quantum gates. Quantum gates are the building blocks of quantum circuits.

Just how we use logic gates in classical computers, we use qubits as quantum gates to perform certain operations in a circuit.

Let's look into an example where we are building a very simple quantum circuit using 2 qubits and by applying two quantum gates namely *The Hadamard Gate and the CNOT gate*.

HADAMARD GATE

The Hadamard gate is a single-qubit operation that maps the basis state |0⟩

$$|0\rangle \text{ to } \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

and |1⟩ to

$$\frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

thus creating an equal superposition of the two basis states.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

CNOT GATE

The CNOT gate is two-qubit operation, where the first qubit is usually referred to as the control qubit and the second qubit as the target qubit.

The first bit of a CNOT gate is the "control bit;" the second is the "target bit." The control bit never changes, while the target bit flips if and only if the control bit is 1.

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

The circuit we are going to build will basically perform a hadamard gate to the first qubit and CNOT gate to both qubits.

The algebraic representation of our circuit will be :

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \left(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -11 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

*printing mistake, should be -1 instead of -11

If we solve the algebraic equation using python:

```
# Define spin-up
u = np.matrix([[1],
               [0]])

# Define the initial state vector
psi = np.kron(u,u)

# Define the identity matrix
I = np.matrix([[1, 0],
               [0, 1]])

# Define the Hadamard gate
H = np.matrix([[1, 1],
               [1, -1]])/np.sqrt(2)

# Define the gate XI
HI = np.kron(H, I)

# Define the CNOT gate
CNOT = np.matrix([[1, 0, 0, 0],
                  [0, 1, 0, 0],
                  [0, 0, 0, 1],
                  [0, 0, 1, 0]])

# Perform the circuit operations
print(CNOT*HI*psi)
```

```
[[0.70710678]
 [0.        ]
 [0.        ]
 [0.70710678]]
```

This outputs the state vector that results from running the quantum circuit we constructed as:

$$|\psi\rangle = \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 1/\sqrt{2} \end{pmatrix}$$

Now, the state vector that we have just constructed exhibits entanglement as well as superposition.
It exists in a combination of two states at once, unlike classical bits which are always zeros and ones.

ANALOGIES

76. Parth Zarekar

ONION ANALOGY

- QC is like a particular case of chopping onions.
- You could peel each layer of onion and *then* chop each layer separately to end up with your result. Or, you could hold the entire thing and run your knife through all the layers so that you essentially “act on all the layers at once” to get your result.

The connection is that quantum computers allow you to perform operations on a whole bunch of input values *simultaneously.* This saves a humongous amount of time for tasks that would otherwise take literally longer than the lifetime of the observable universe if you rather went on operating on one input at a time.

FOOTBALL ANALOGY

In soccer, players generally cannot use their hands. As a result of this rule, the sport looks a certain way, with athletes mostly using their feet to control and kick the ball.

- Now if the rules were changed so that players could use their hands, soccer would look very different. In some cases, it would be faster or easier for athletes to use their hands to hold, throw, or catch the ball. In other cases, however, it would still be better to kick the ball.
- For example, most soccer players can kick the ball across the field faster than they can throw the ball or run with it. So, to get the ball across the field as quickly as possible, it may still be better to use one’s feet.

- Analogously, the essence of quantum computing is to change the rules so that a computer can now use its “hands.” That is, the rules of the game are changed from the laws of classical physics to the laws of quantum physics.
- As a result, a quantum computer can solve some problems faster by using its “hands.” For other problems, using one’s “feet” is better, so a quantum computer is no faster for these problems.

CONCEPTS AND PHYSICAL MANIFESTATION

54. Krishnaraj

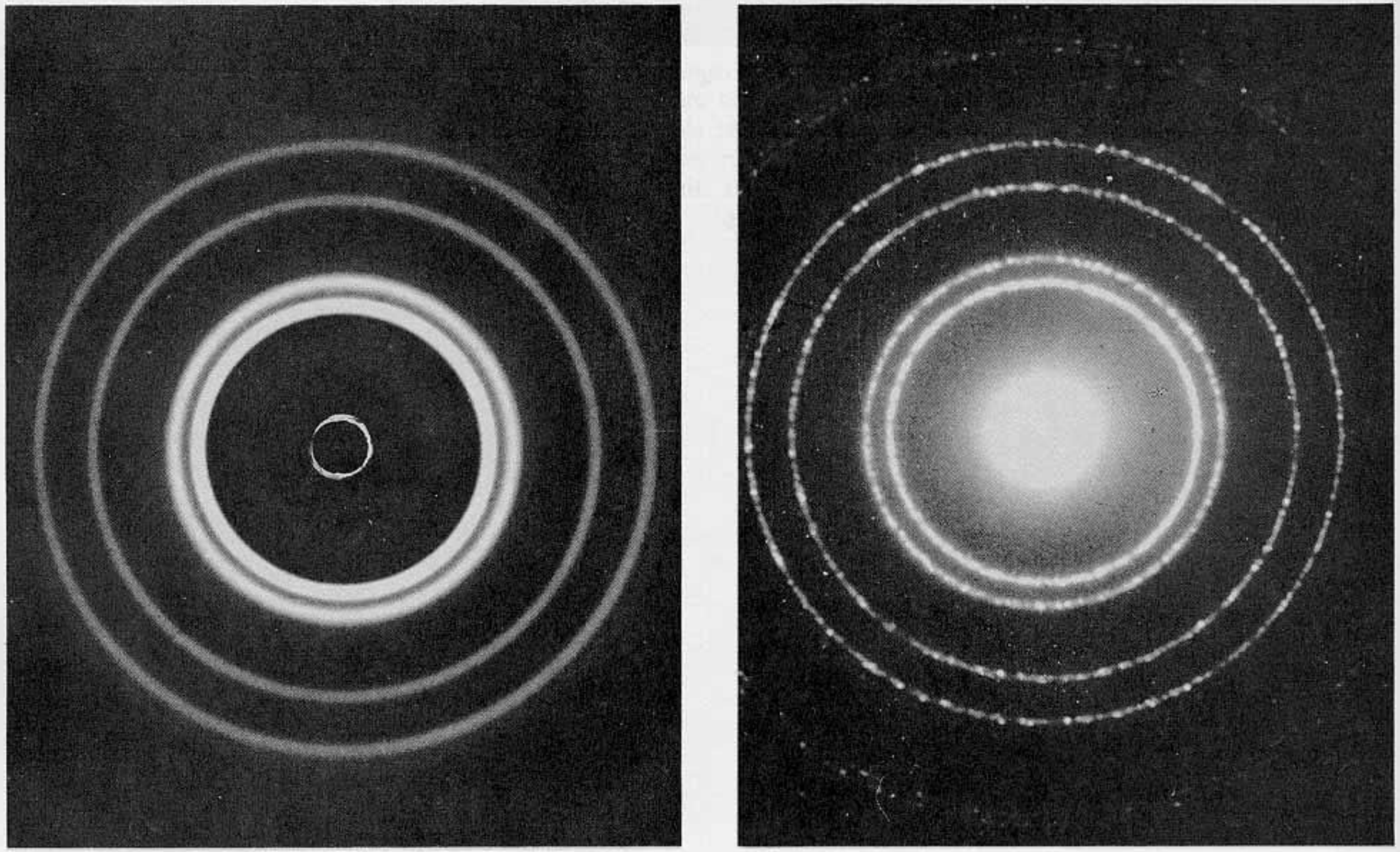
SUPERPOSITION

- Quantum superposition is a fundamental principle of quantum mechanics. It states that, much like waves in classical physics, any two (or more) quantum states can be added together ("superposed") and the result will be another valid quantum state; and conversely, that every quantum state can be represented as a sum of two or more other distinct states.
- Mathematically, it refers to a property of solutions to the Schrödinger equation; since the Schrödinger equation is linear, any linear combination of solutions will also be a solution.

ELECTRON BEAM

An example of a physically observable manifestation of the wave nature of quantum systems is the interference peaks from an electron beam in a double-slit experiment. The pattern is very similar to the one obtained by diffraction of classical waves.

The diffraction pattern on the left was made by a beam of x rays passing through thin aluminum foil. The diffraction pattern on the right was made by a beam of electrons passing through the same foil.



WHY IS IT IMPORTANT HERE?

Through superposition, an amount of *N* qubits can express the same amount of information as 2^*N* classical bits, although this informational richness is not accessible to us because the *N* qubits will "collapse" back to behave like *N* classical bits when measured.

But before that, while still in their (unobserved) state of quantum superposition, 2 qubits can be in the same amount of states as 4 classical bits, 4 qubits the same as 16 bits, 16 qubits the same as 65,536 bits, and so on.

QUANTUM SUPREMACY

A system of 300 qubits can reflect more states than there are atoms in the universe. A computer based on bits could never process that amount of information, which is why quantum computing represents a true “quantum leap” in terms of capability.

ENTANGLEMENT

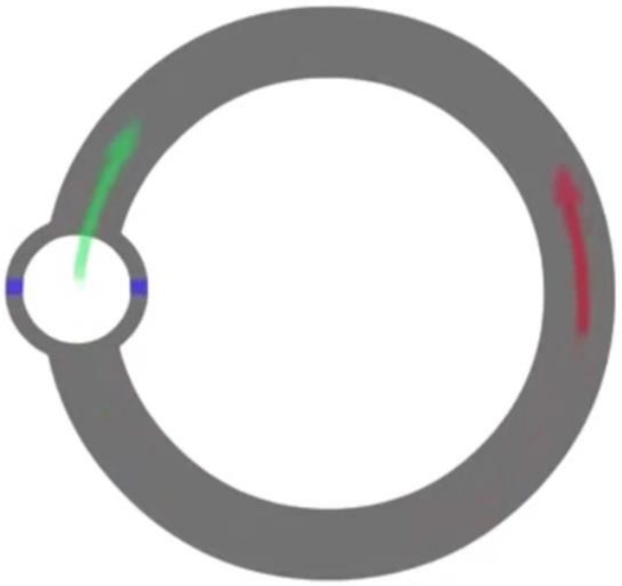
Even more surprising than superposition, quantum theory predicts that entities may have correlated fates. That is, the result of a measurement on one photon or atom leads instantaneously to a
correlated result when an entangled photon or atom is measured

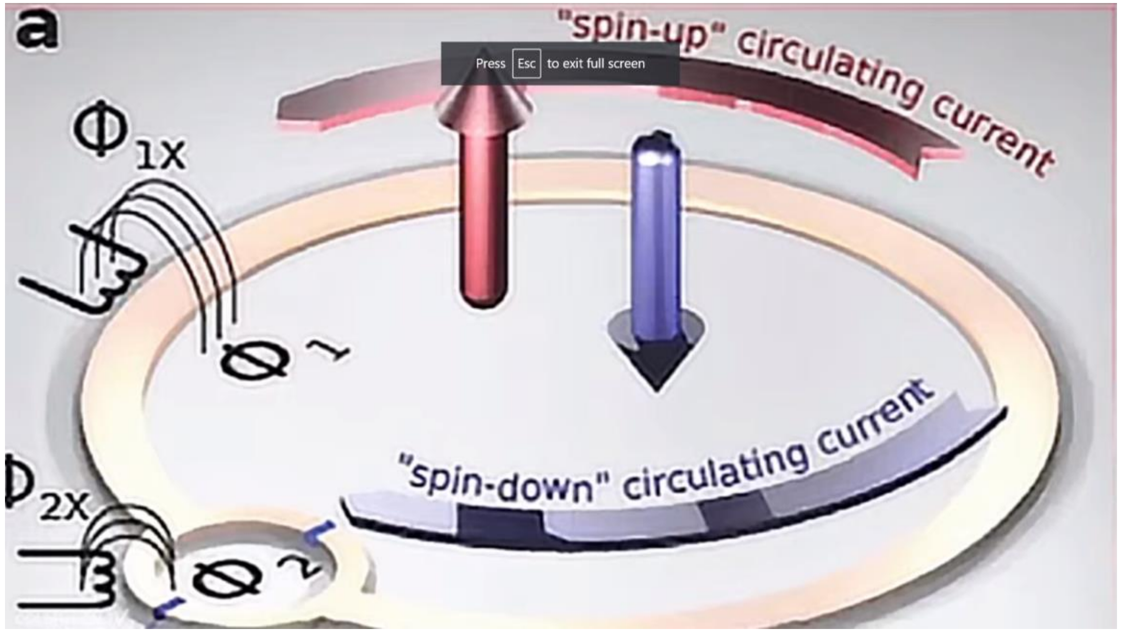
THE ENTANGLED COINS

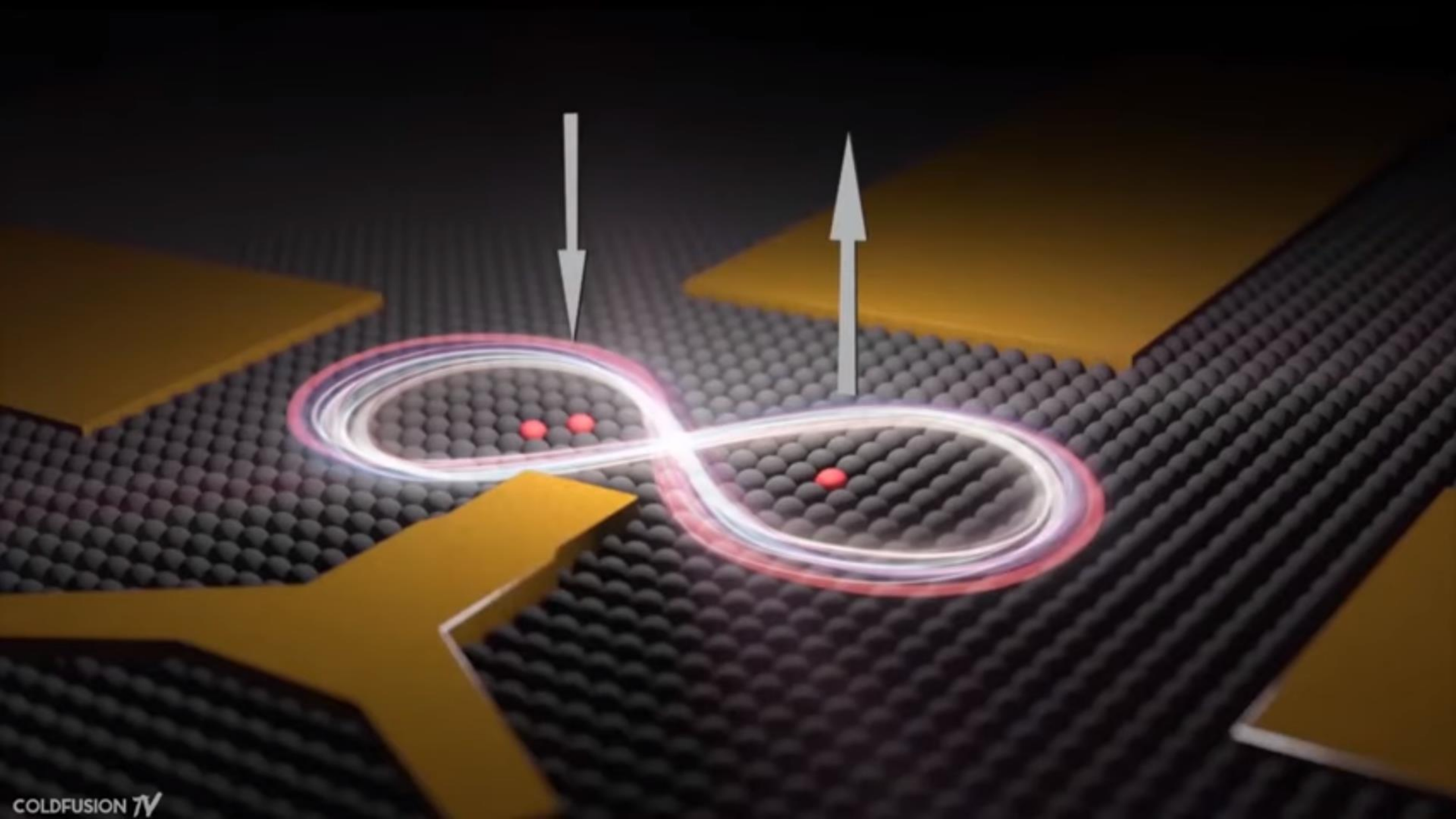
For a more intuitive grasp of what we mean by "correlated results," imagine that two coins could be entangled. Imagine one is tossing a coin.

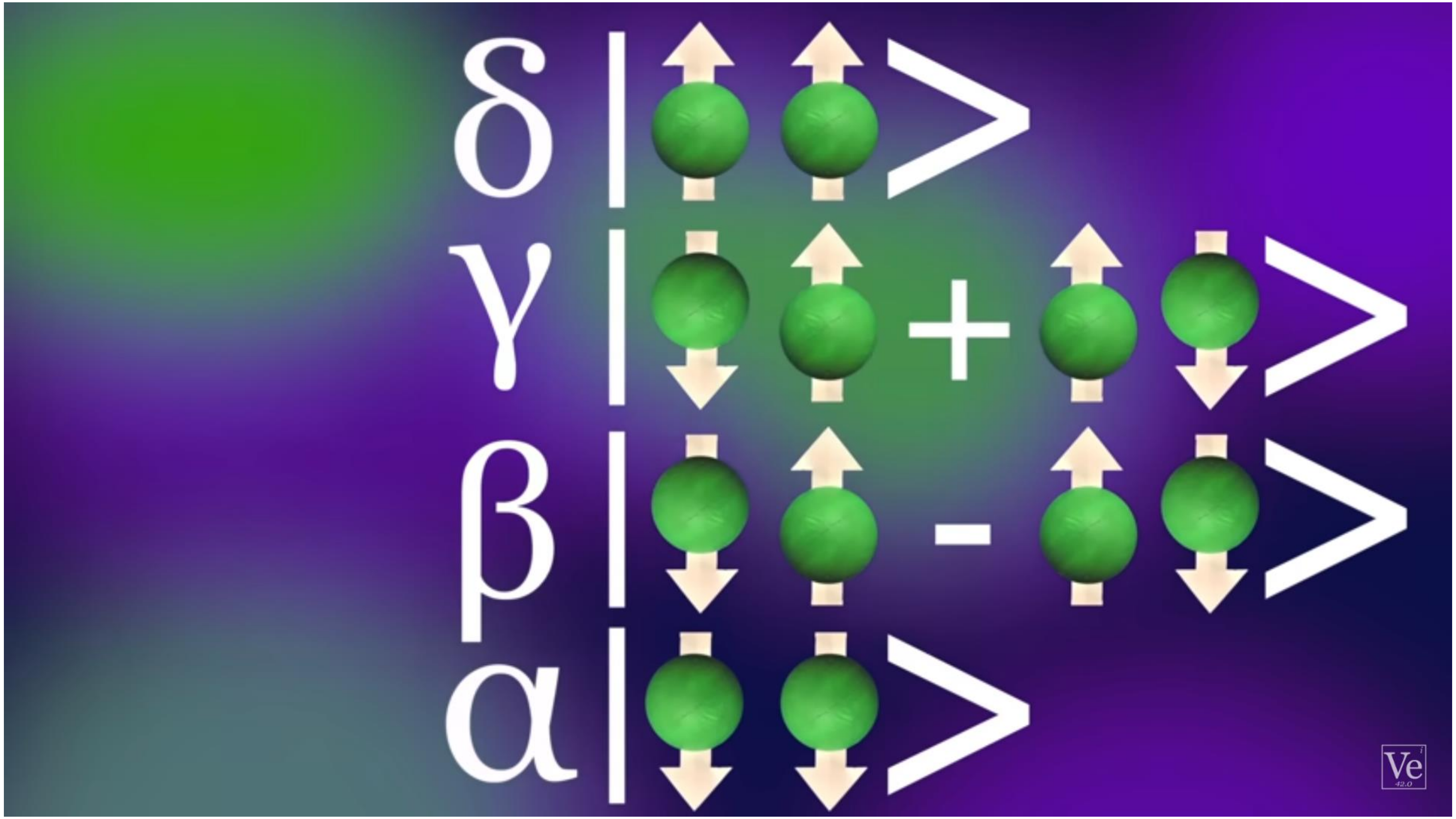
WHAT THOSE QUBITS LOOK LIKE

1. Superconductivity
2. Quantum Dots




a
"spin-up" circulating current
Press Esc to exit full screen
Φ_{1X}
Φ_{2X}
"spin-down" circulating current

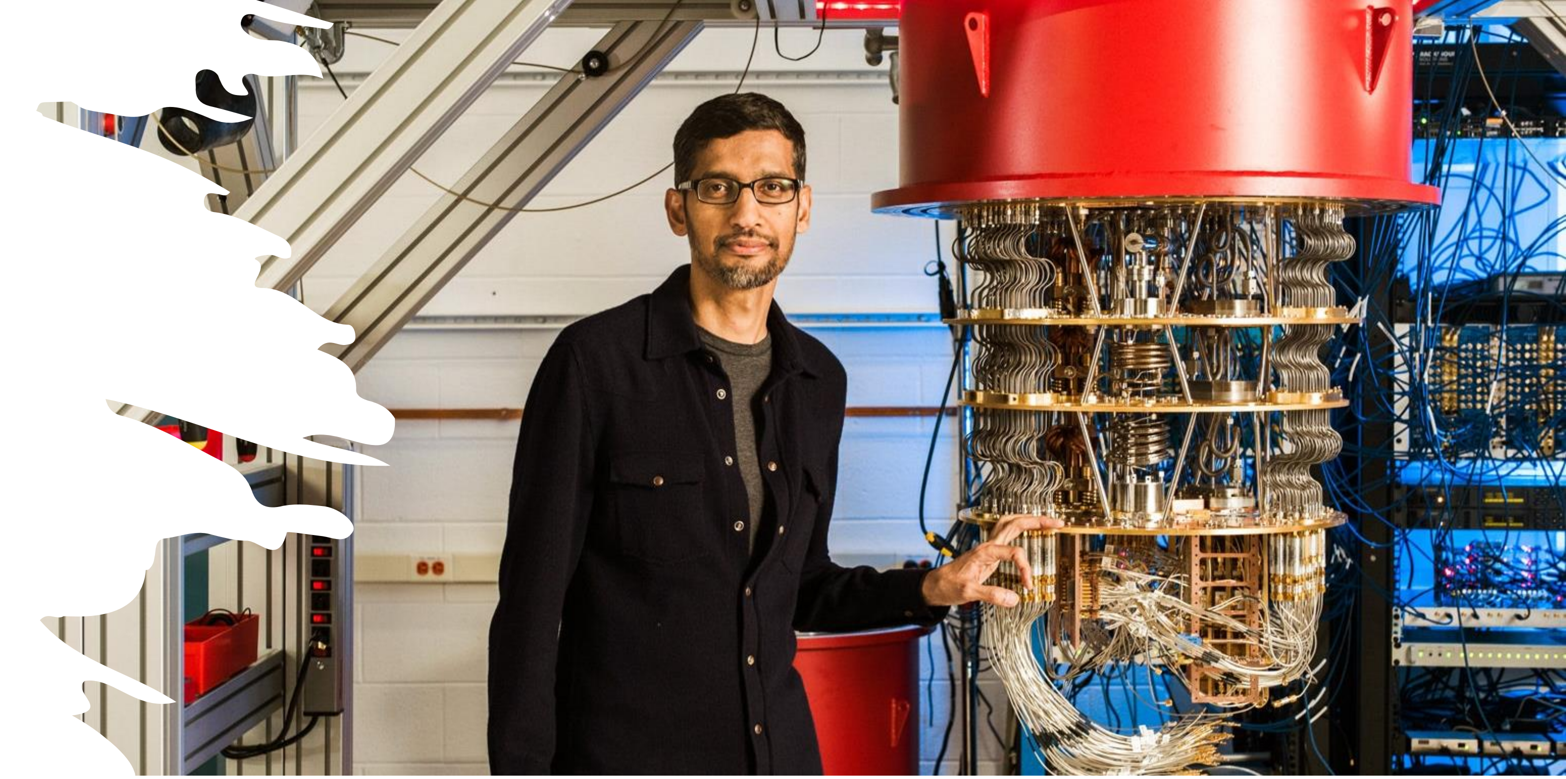


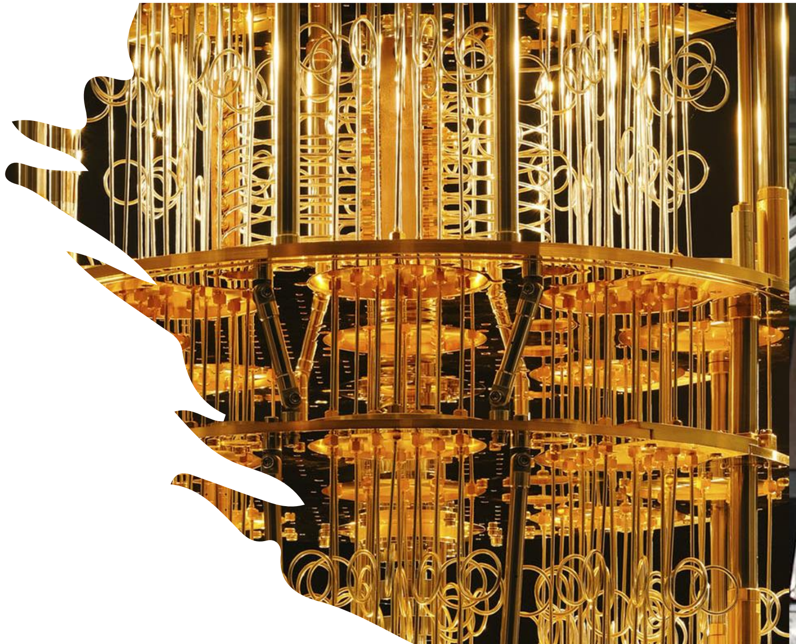


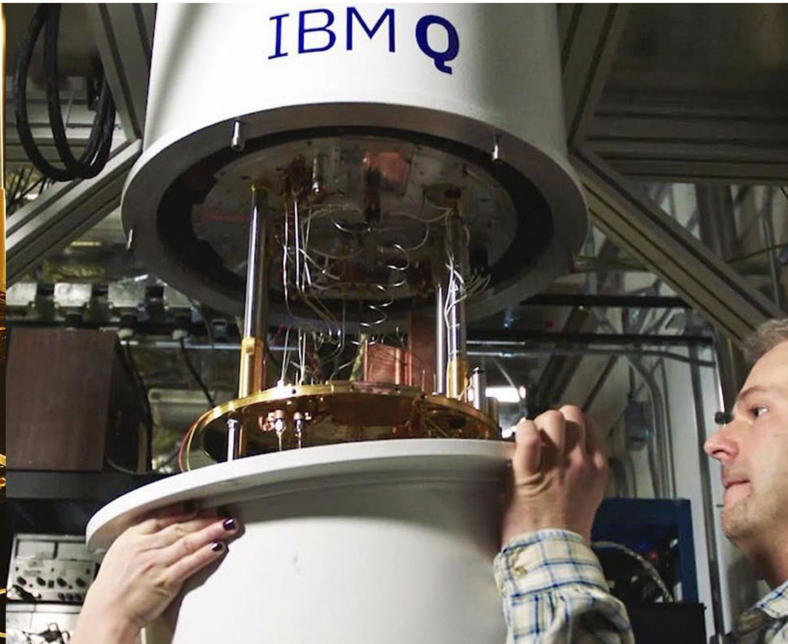
HOW A SINGLE QUBIT IS WORTH 2 BITS

IBM and Google's Quantum Computers

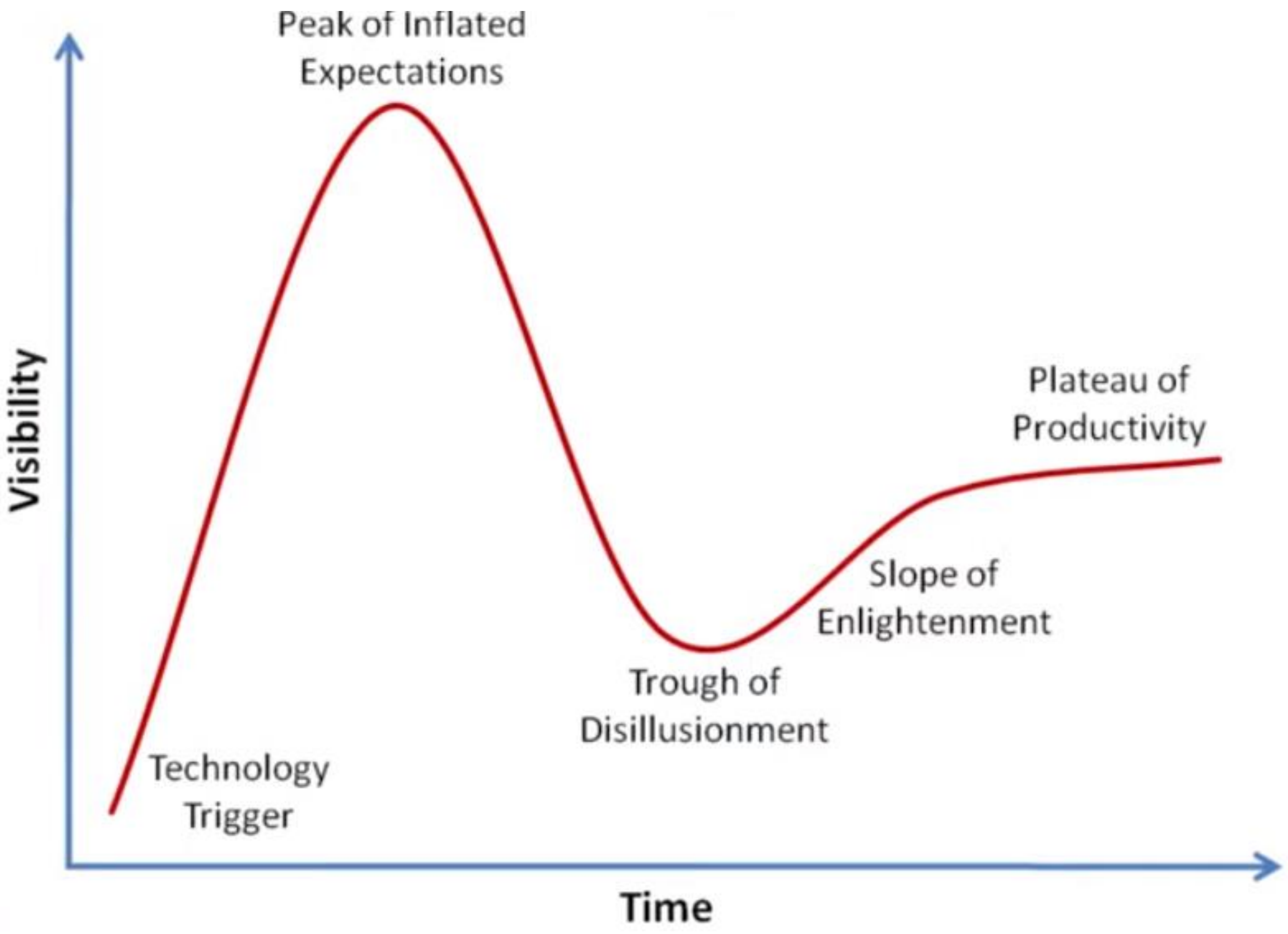
These use superconducting transmon qubits made from superconducting materials such as niobium and aluminium.







DEVELOPMENT GRAPH



APPLICATIONS ON WEATHER FORECASTINGAND FINANCIAL MODELLING

50. Atharva Tanawade

WEATHER FORECASTING

Every year there are hurricanes, extreme heat waves, tornadoes, and other extreme weather events, resulting in thousands of deaths and billions of dollars in damages. Prediction of extreme weather further in advance and with increased accuracy could allow for targeted regions to be better prepared in order to reduce loss of life and property damage.

Quantum computing has the potential to improve conventional numerical methods to boost tracking and predictions of meteorological conditions by handling huge amounts of data containing many variables efficiently and quickly, by harnessing the computing power of qubits, and by using quantum-inspired optimization algorithms. Moreover, pattern recognition, crucial for understanding the weather, can be enhanced by means of quantum machine learning.

APPLICATION IN FINANCE

Any financial services activities, from securities pricing to portfolio optimization, require the ability to assess a range of potential outcomes. To do this, banks use algorithms and models that calculate statistical probabilities. These are fairly effective but are not infallible, as was shown during the financial crisis a decade ago, when apparently low-probability events occurred more frequently than expected.

In a data-heavy world, ever-more powerful computers are essential to calculating probabilities accurately. With that in mind, several banks are turning to a new generation of processors that leverage the principles of quantum physics to crunch vast amounts of data at superfast speed.

Google, a leader in the field, said in 2019 that its Sycamore quantum processor took a little more than three minutes to perform a task that would occupy a supercomputer for thousands of years. T

he experiment was subject to caveats but effectively demonstrated quantum computing’s potential, which in relative terms is off the scale.

Quantum computers are particularly promising where algorithms are powered by live data streams, such as real-time equity prices, which carry a high level of random noise.

Other financial Applications

- Business optimization, including risk management and compliance.
- Quantum computing's specific use cases for financial services can be classified into three main categories: targeting and prediction, trading optimization, and risk profiling.
- We explore potential use cases in each of these categories, providing examples that apply to three main industries in financial services: banking, financial markets, and insurance.

44. Devanshu Surana

APPLICATIONS ON CRYPTOGRAPHY, DRUGS AND AI AND ML

CRYPTOGRAPHY

Cryptography is the process of encrypting data, or converting plain text into scrambled text so that only someone who has the right “key” can read it. Quantum cryptography, by extension, simply uses the principles of quantum mechanics to encrypt data and transmit it in a way that cannot be hacked.

Quantum cryptography uses a series of photons (light particles) to transmit data from one location to another over a fiber optic cable. By comparing measurements of the properties of a fraction of these photons, the two endpoints can determine what the key is and if it is safe to use.

APPLICATION IN AI

Quantum computing can be used for the rapid training of machine learning models and to create optimized algorithms. An optimized and stable AI provided by quantum computing can complete years of analysis in a short time and lead to advances in technology.

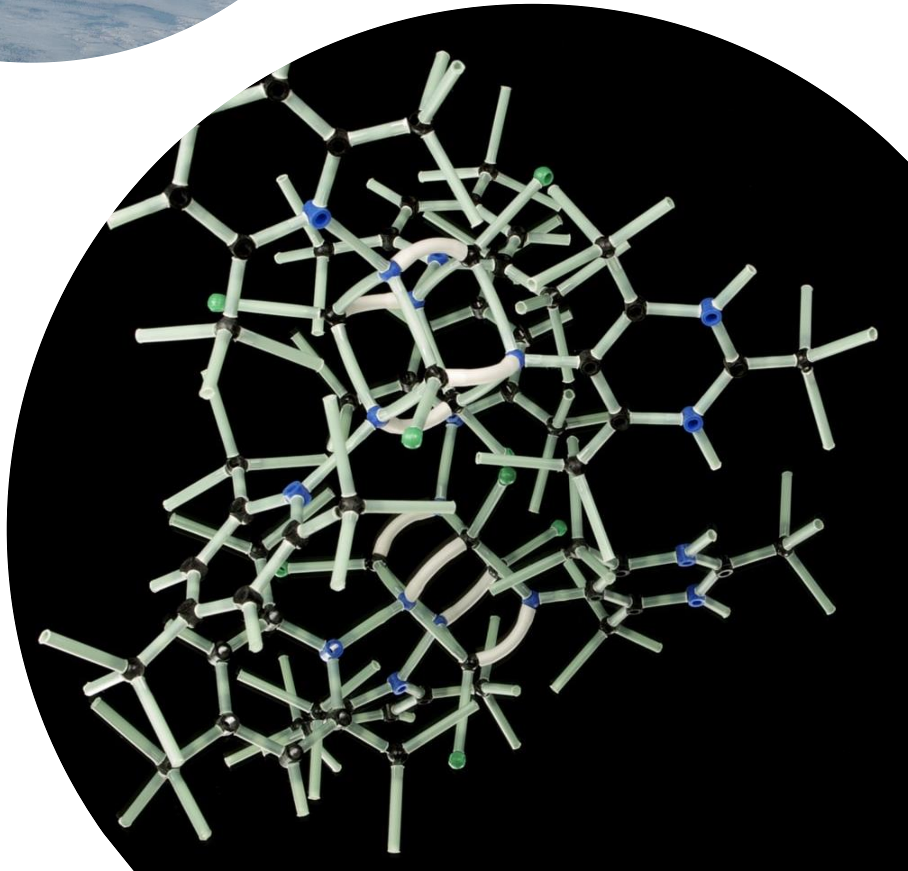
Quantum computing opens the door potentially solving very large and complex computational problems that are basically impossible to solve on traditional computers. This includes things like using brute-force methods to guess the passcode used to encrypt a piece of data using a 256-bit algorithm.

APPLICATION IN MACHINE LEARNING

- If quantum computers have speedups in linear algebra subroutines, it can speed up machine learning.
- Quantum parallelism can help train models more faster

Here are a few examples of where quantum machine learning will have an effect:

- Understanding nanoparticles
- Making novel materials using molecular and atomic mapping
- Molecular modeling for drug discovery and medical research
- Knowing the human body's deeper structure
- Pattern recognition and classification have been improved.
- Advancing space exploration



DRUG DESIGN AND DEVELOPMENT

- In the healthcare industry, quantum computing could enable a range of disruptive use cases for providers and health plans by accelerating diagnoses, personalizing medicine, and optimizing pricing. Quantum-enhanced machine learning algorithms are particularly relevant to the sector.
- Pharma is a natural contender for quantum computing because it concentrates on molecule formations. The molecules (including those that may be utilized to make medicines) are quantum systems or systems based on quantum physics.
- Quantum Computing is predicted to be more successful than traditional computers at predicting and simulating the structure, characteristics, and behavior (or reactivity) of these molecules.

GROUP MEMBERS

44. Devanshu Surana
49. Varad Talegaonkar
50. Atharva Tanawade
54. Krishnaraj Thadesar
76. Parth Zarekar
71. Pranav Walvekar


Thank You!