Quantum Computing

- SCIENCE OR FICTION ?

Preben Thorö

2021-JUN-10

TRIFORK.
...think software

Me

- CTO
- International Speaker
- Head of Trifork's GOTO Conference Program Committees
- Product Manager
- Coach
- Senior Developer
- Professional and Spare Time Nerd
- Almost ended up as a quantum physisit…

Opening Question

Quantum computing: Is it science fiction?

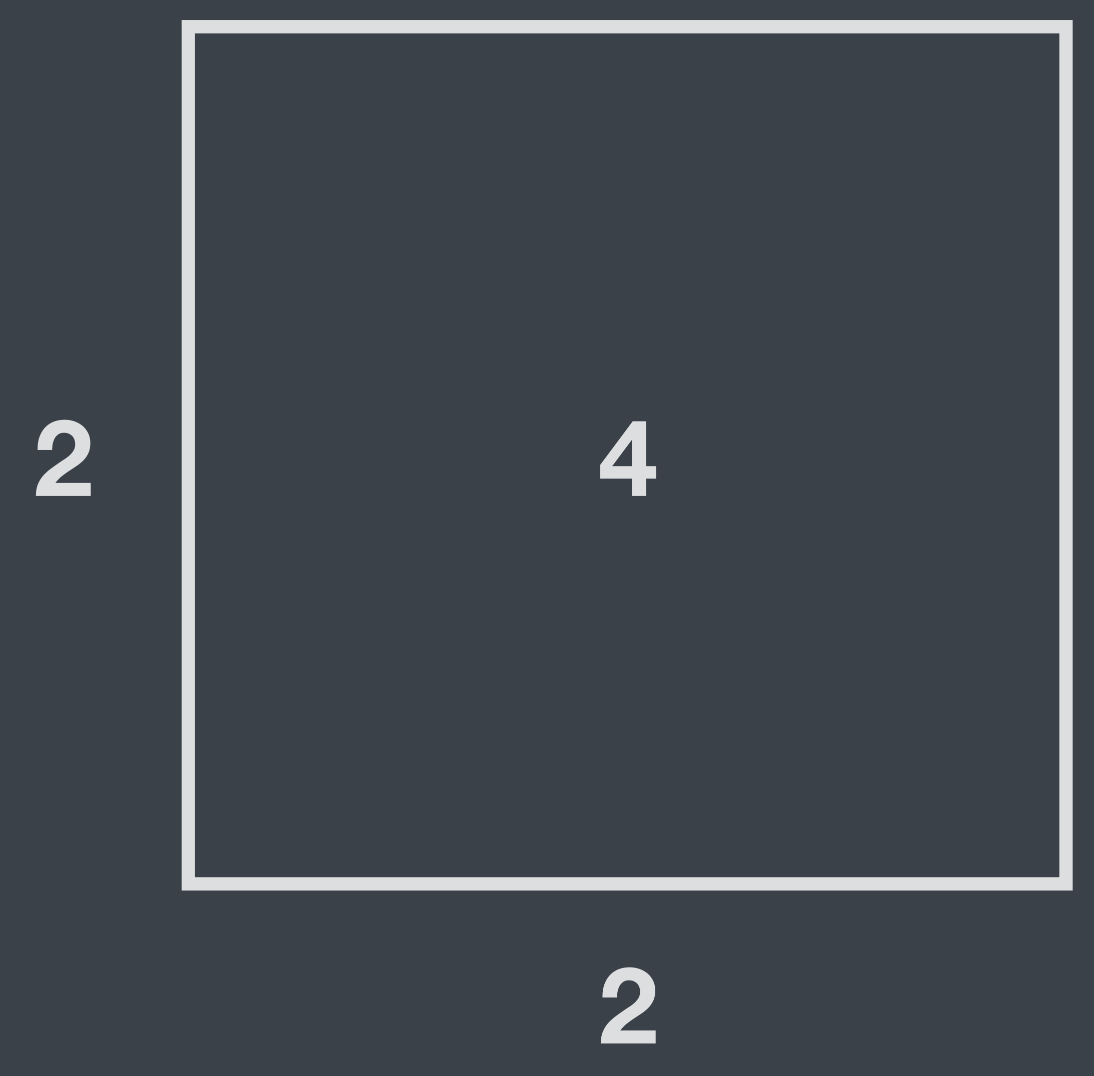
Complex Numbers

Who can really claim that they understand complex numbers?

- that numbers in the nature are in fact two-dimensional ? (or more correct: that two dimensional numbers seem to describe the world around us)

Complex Numbers

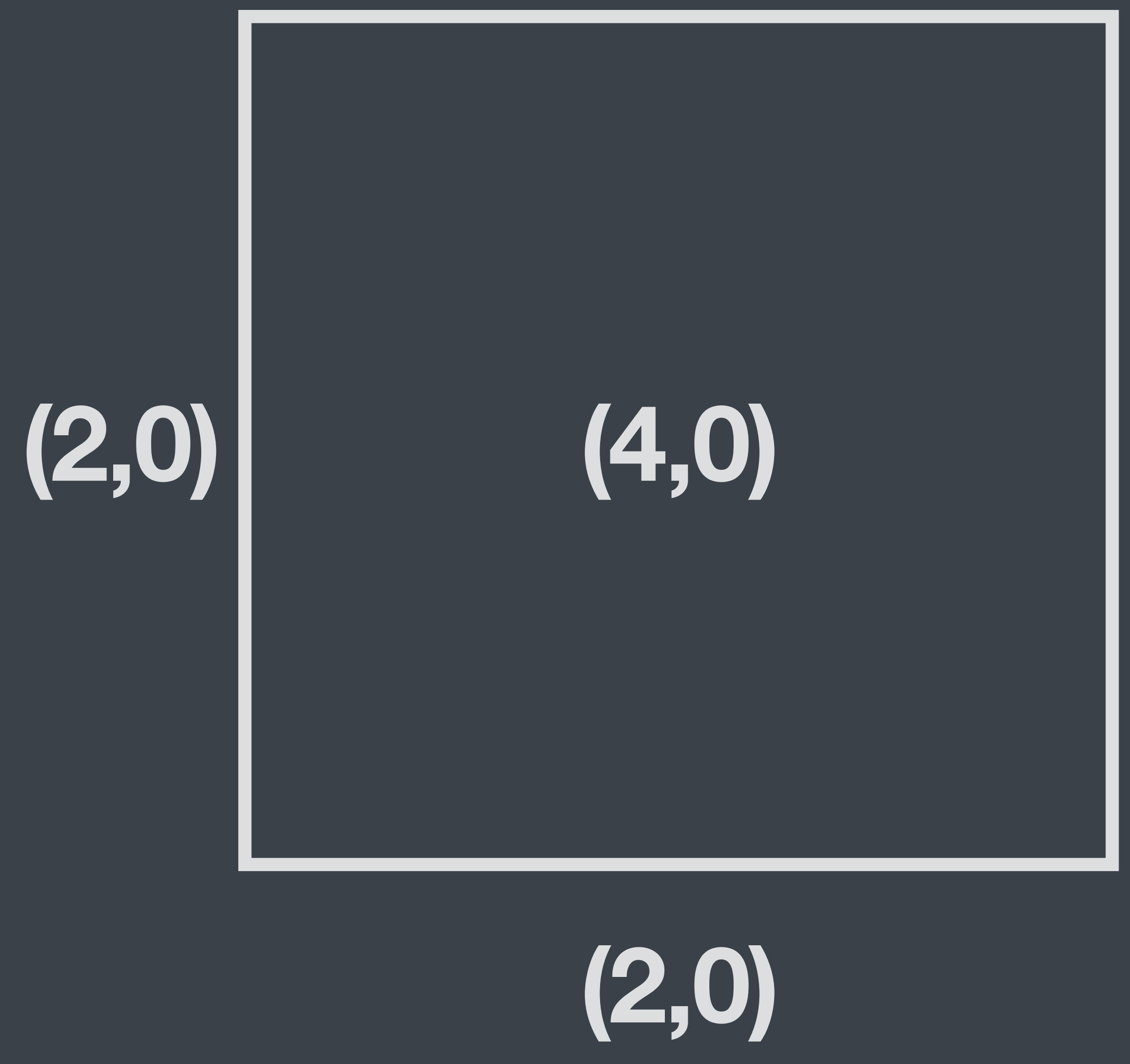
Who can really claim that they understand complex numbers?



$2 \times 2 = 4$

Complex Numbers

Who can really claim that they understand complex numbers?



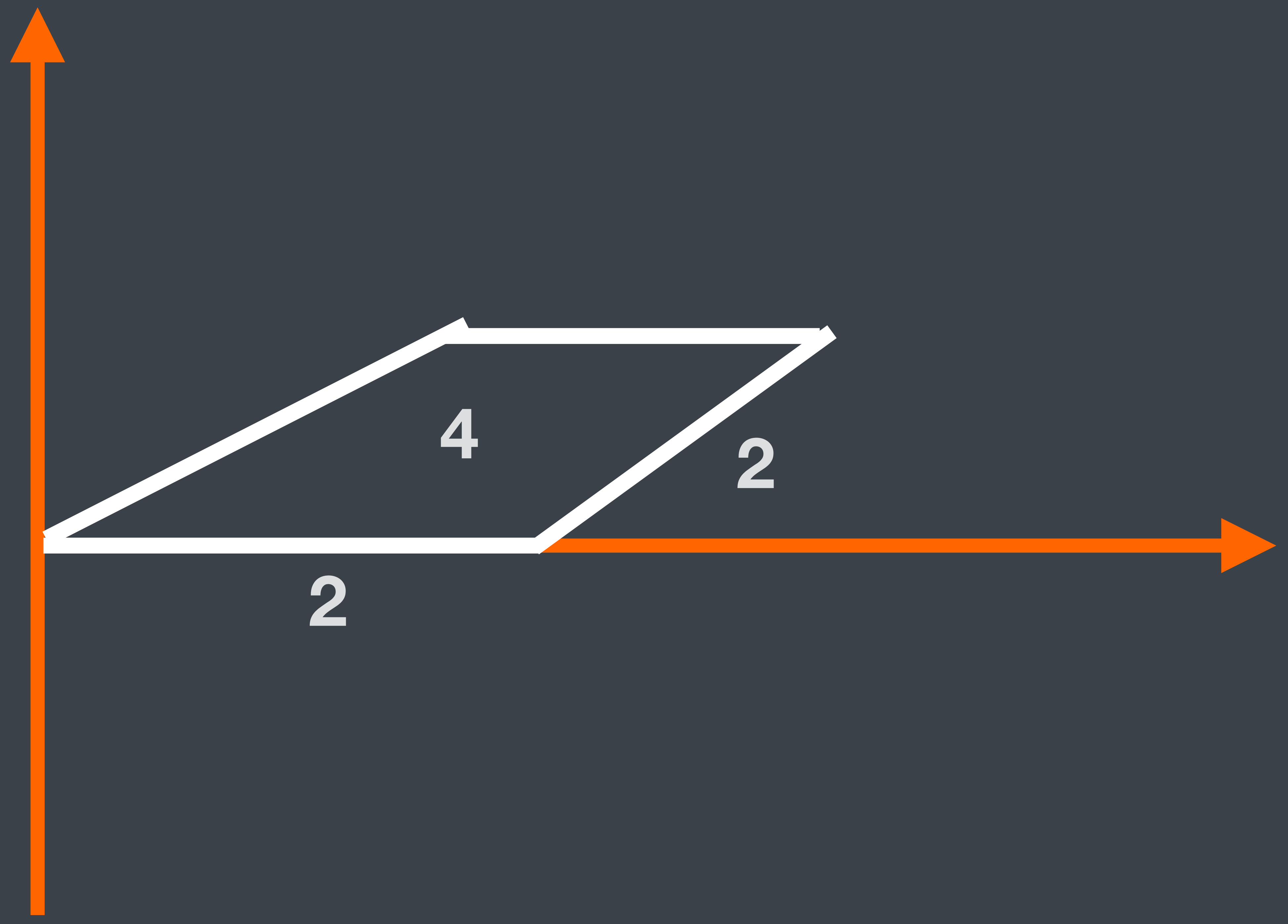
(2,0) x (2,0) = (4,0)

Complex Numbers

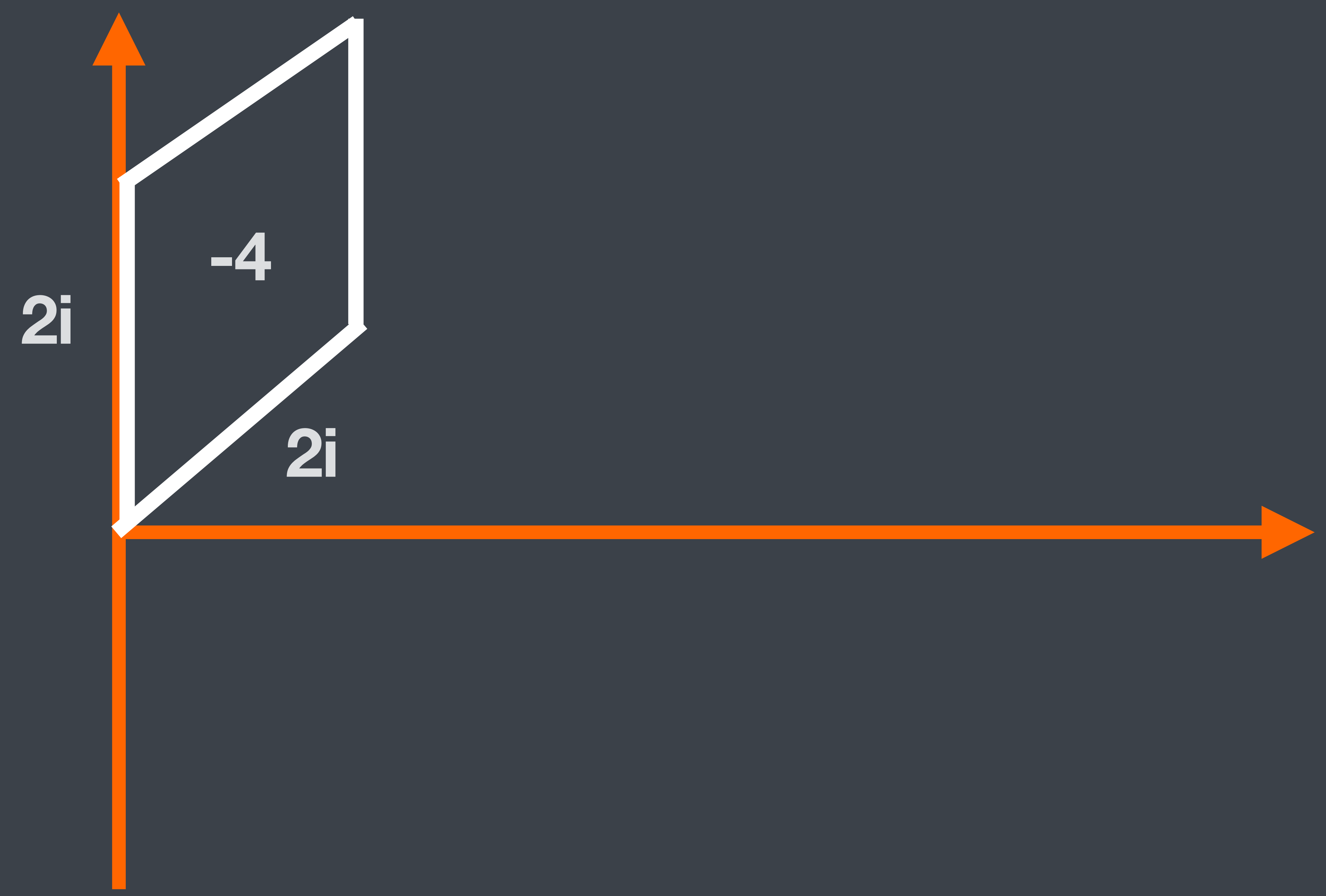
Who can really claim that they understand complex numbers?

(0,2) x (0,2) = -4

Complex Numbers



Complex Numbers



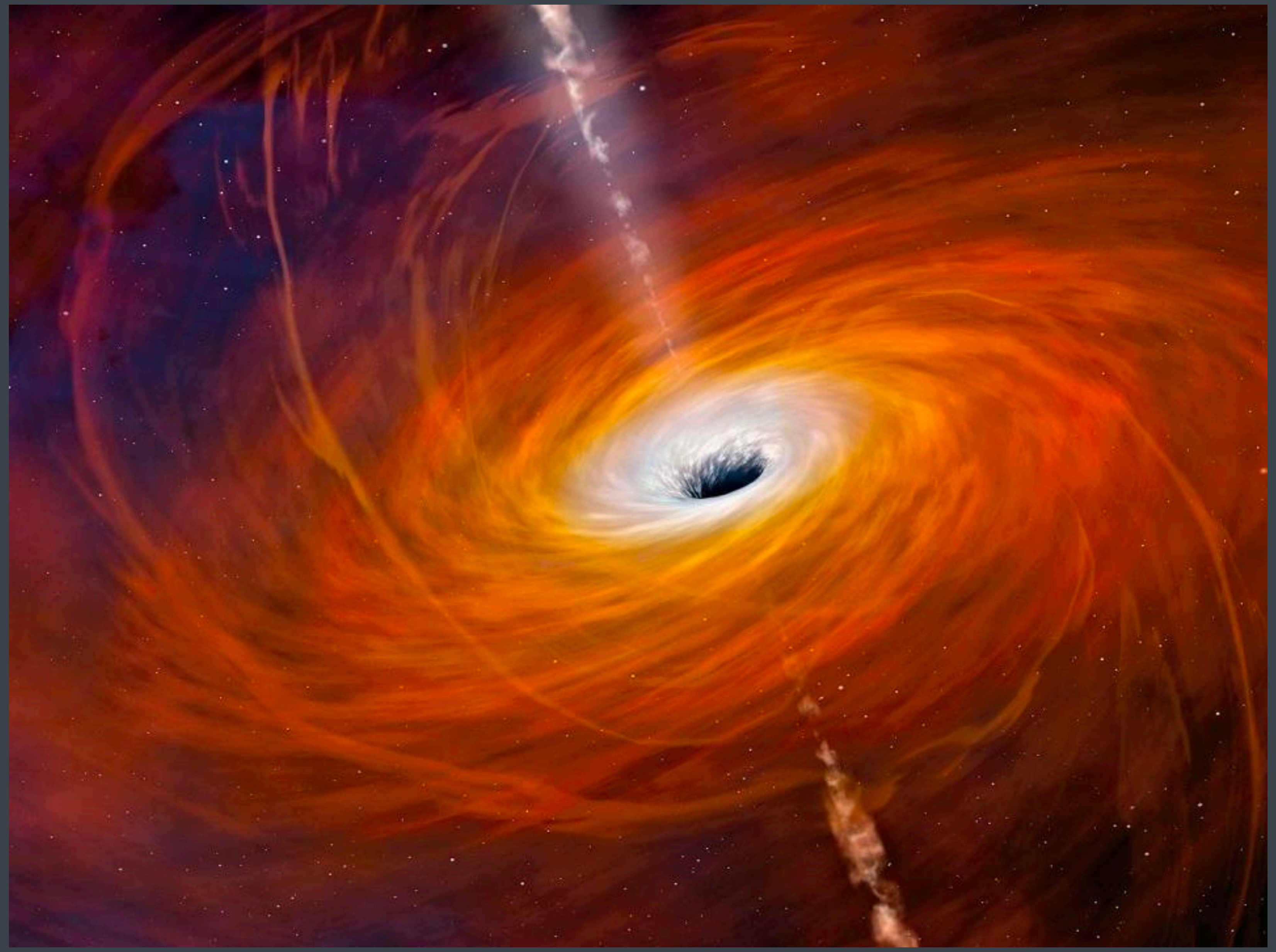
Complex Numbers

It gets even worse when time becomes two dimensional…

How do we grasp that time is not a straight line
in one dimension ?

Complex Numbers

But it helps us understand the physics of black holes (though it is hard to understand that they vaporize into imaginary time)



(from forbes.com)

Complex Numbers

$$a_1 \cdot \frac{dy}{dt} + a_0 \cdot y(t) = b_0 \cdot u(t)$$

$$\Downarrow$$

$$s \cdot Y(s) - y(0) + a_0 \cdot Y(s) = b_0 \cdot U(s)$$

Complex Numbers

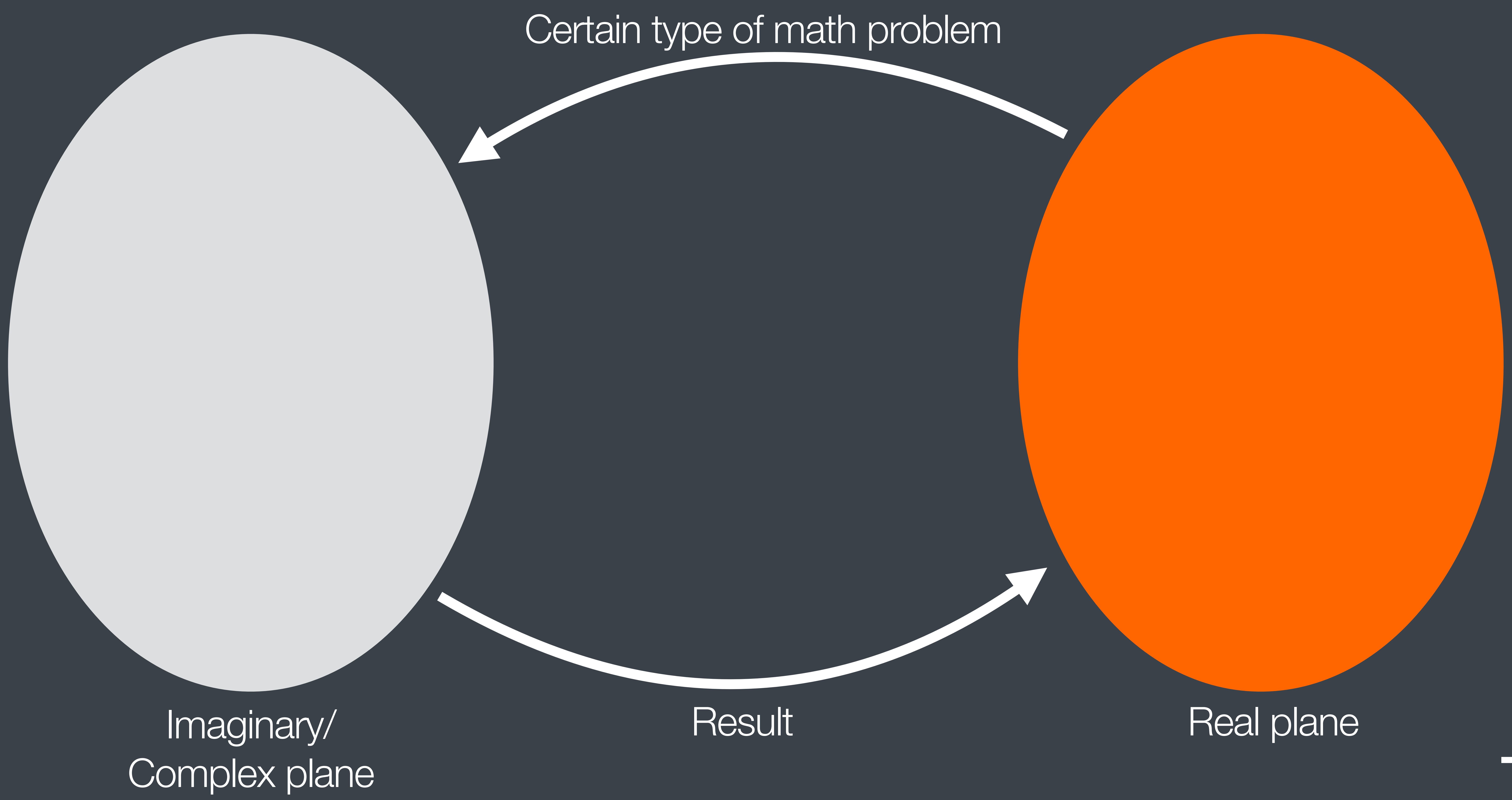
$$\cosh(at) \cdot f(t)$$

$$\downarrow$$

$$\frac{1}{2} \cdot (F(s-a) + F(s+a))$$

TRIFORK.
...think software

Complex Numbers



TRIFORK.
...think software

Complex Numbers

(from elsikkerhetsportalen.no)

(from philips.ch)

(from audiovisualsolutionsgroup.com)

Complex Numbers

What is the problem?

Our language and ability to express ourselves has been formed by what we can see, feel, measure, sense…

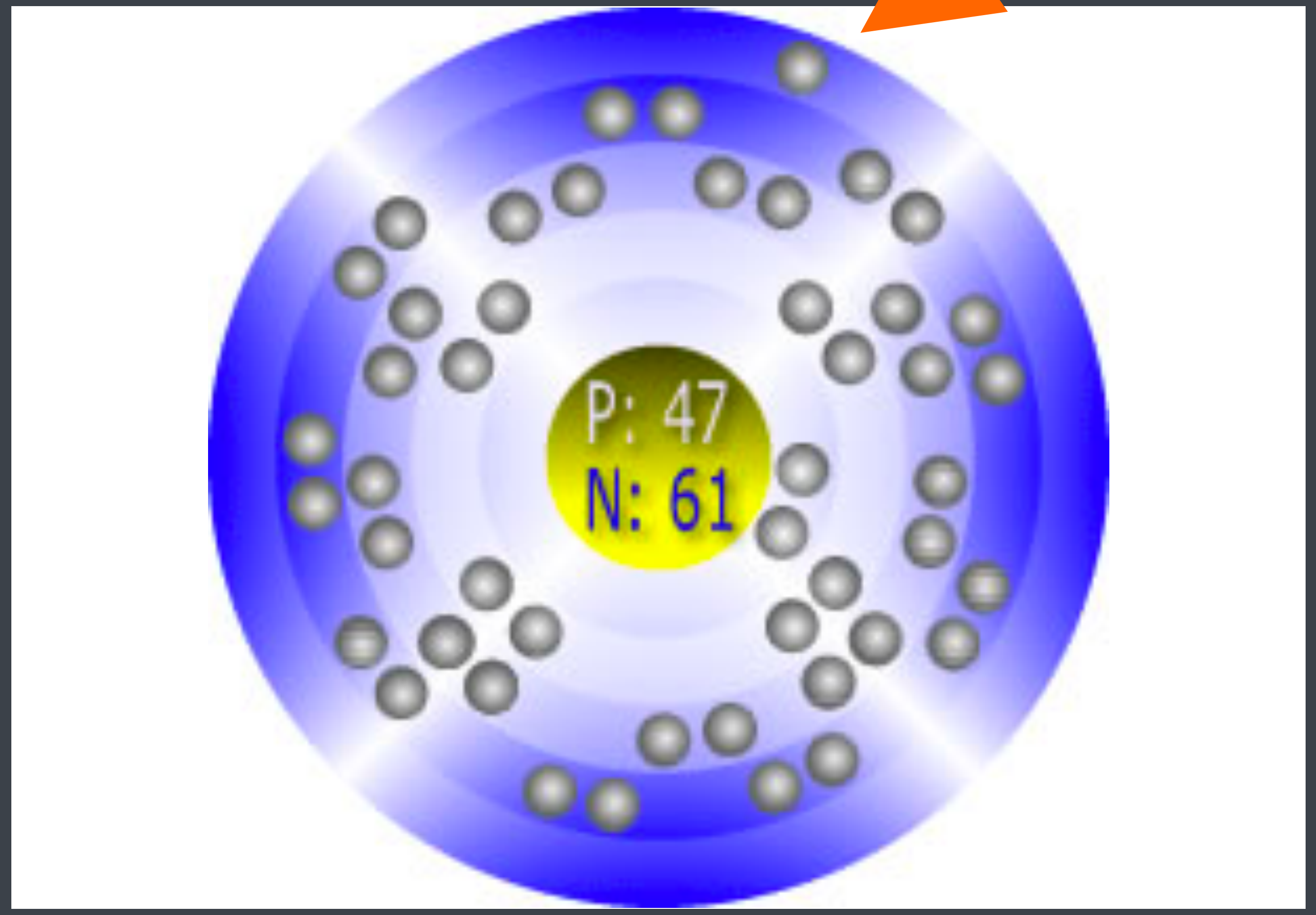
…and we cannot measure two-dimensional time or a negative surface

It becomes academic. We can only describe it through math.

Spinning Atoms

Some atoms become magnetic when they spin (fly around)

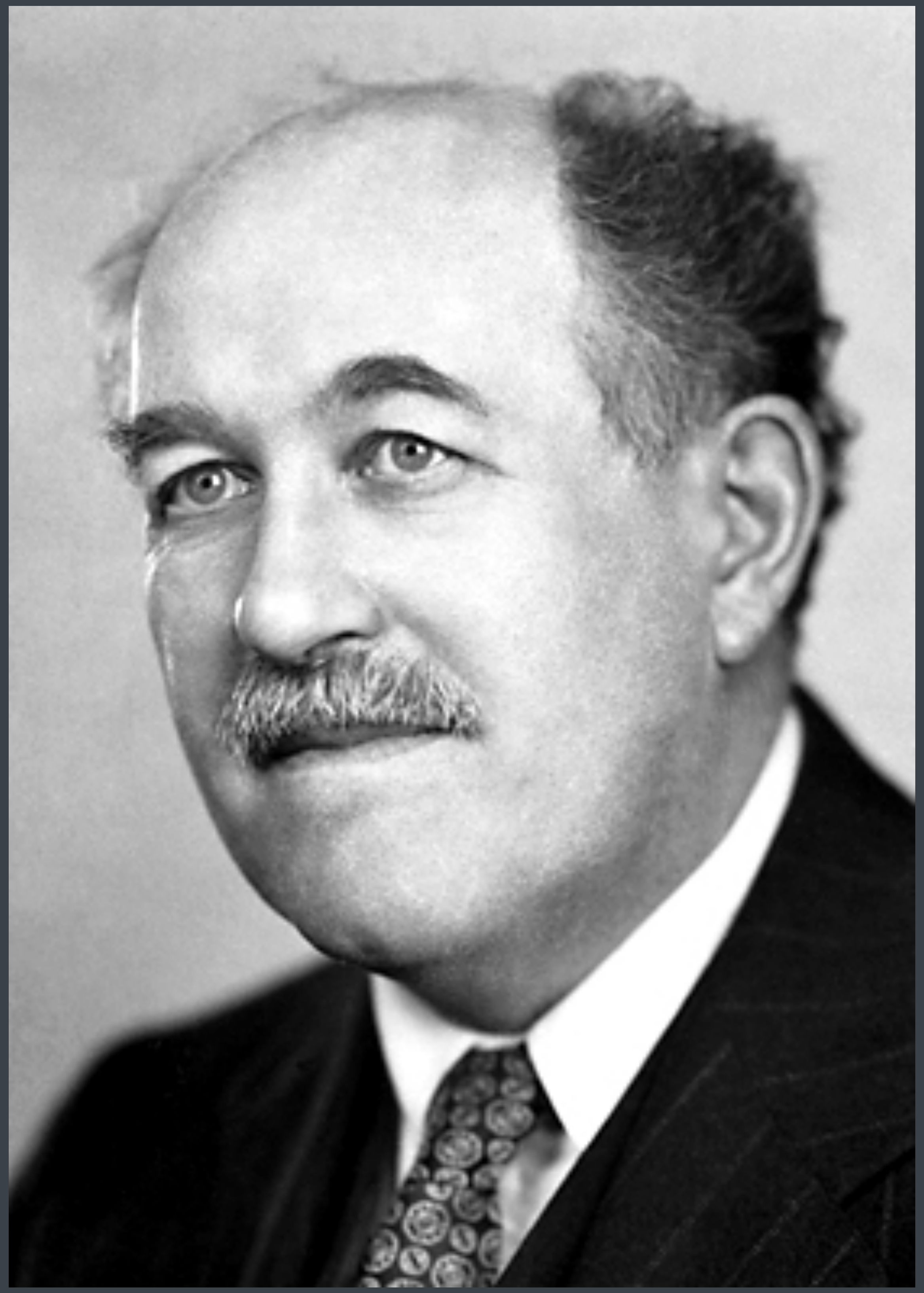
And dependig on the speed and direction of the movement, the resulting magnet can point into any direction



(from silvercoinstoday.com)

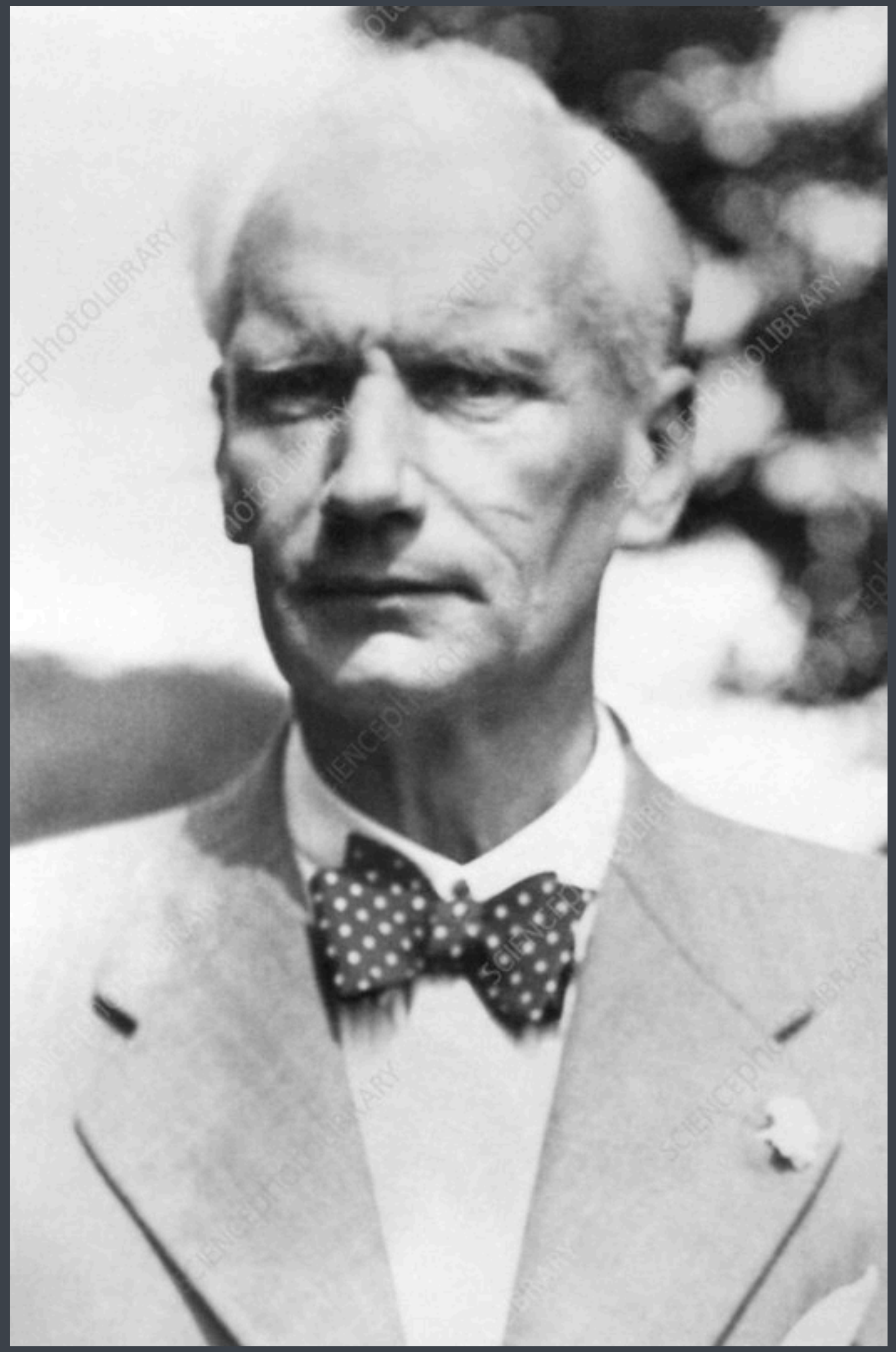
The Stern-Gerlach Experiment

Otto Stern



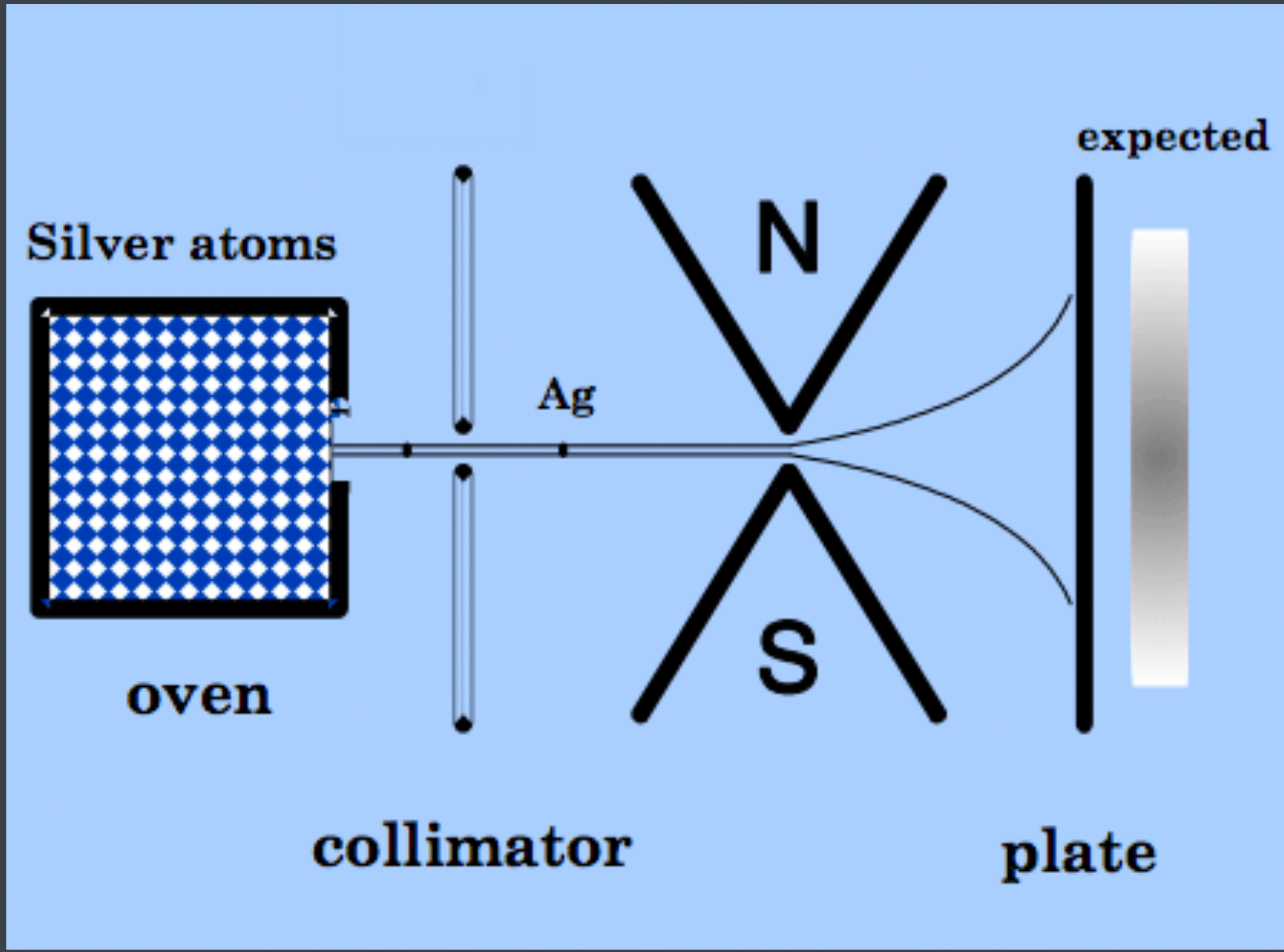
(from Wikipedia)

Walter Gerlach



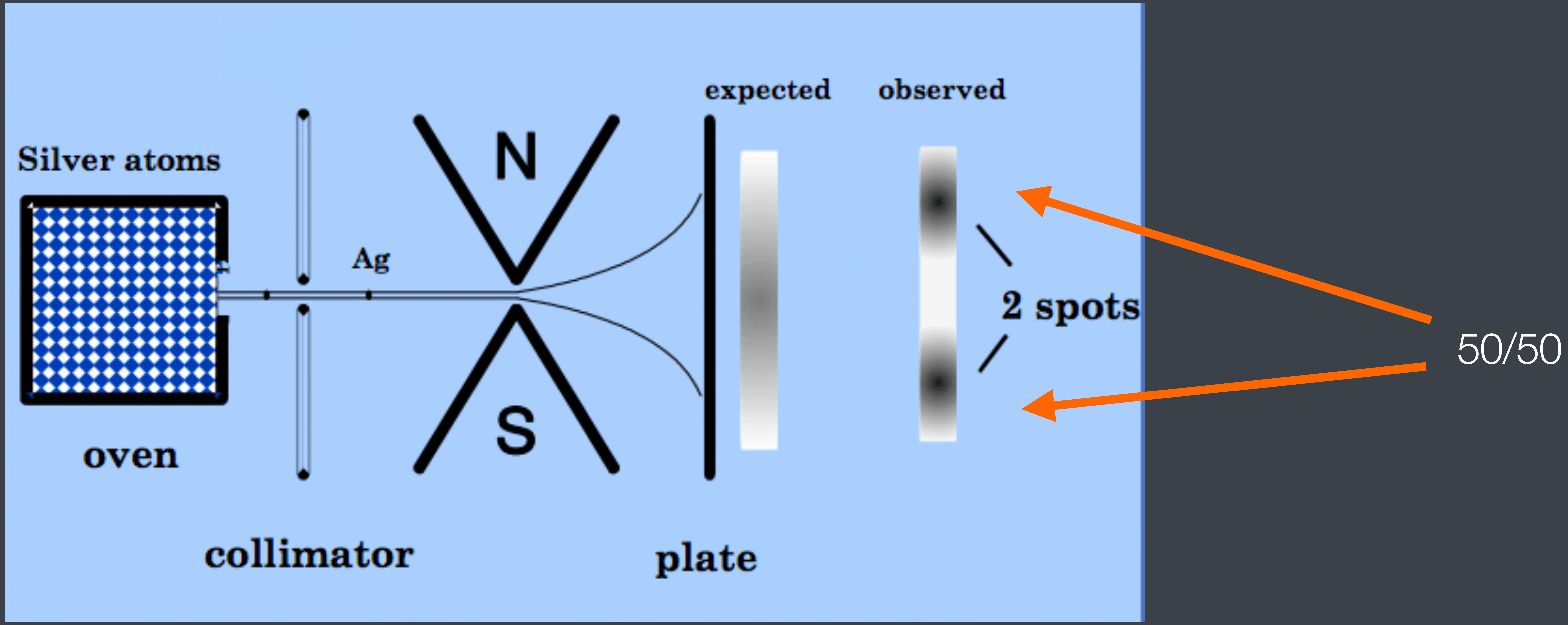
(from sciencephoto.com)

The Stern-Gerlach Experiment



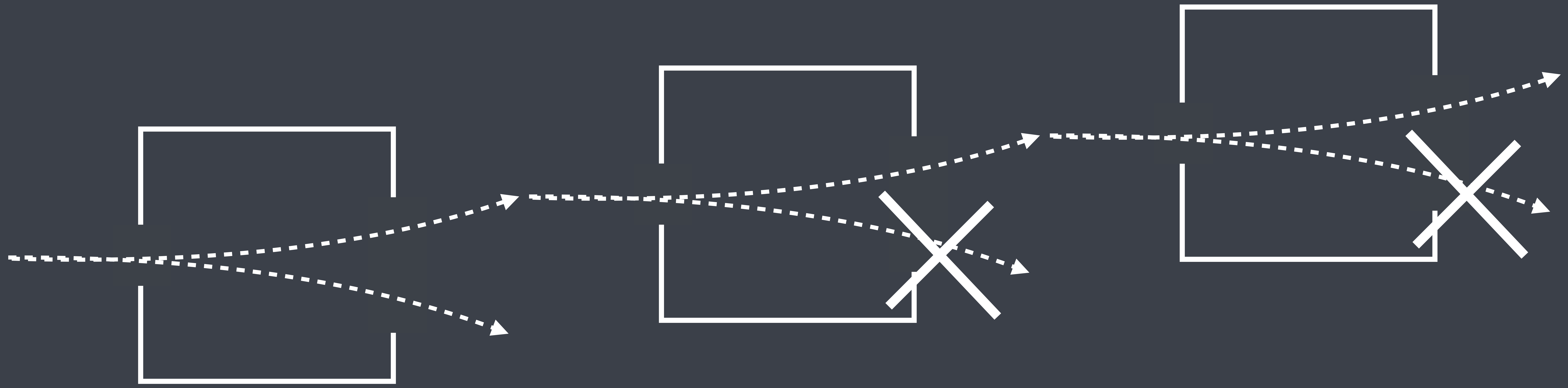
(from mri-q.com)

The Stern-Gerlach Experiment

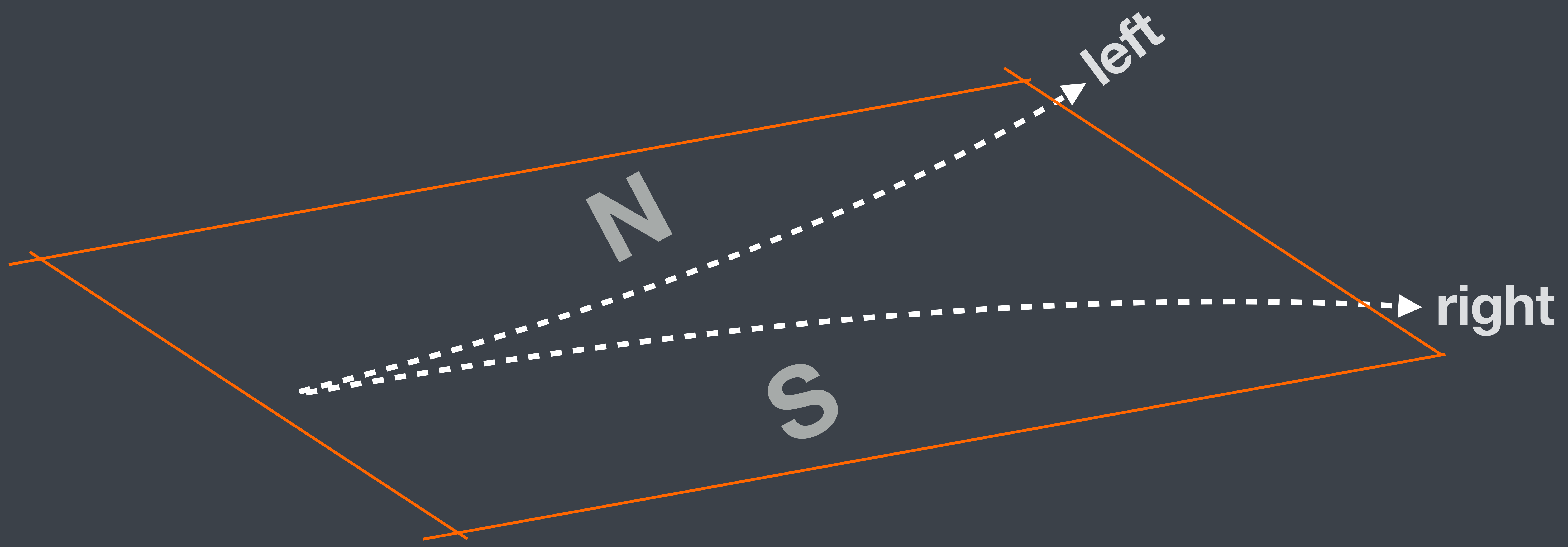


(from mri-q.com)

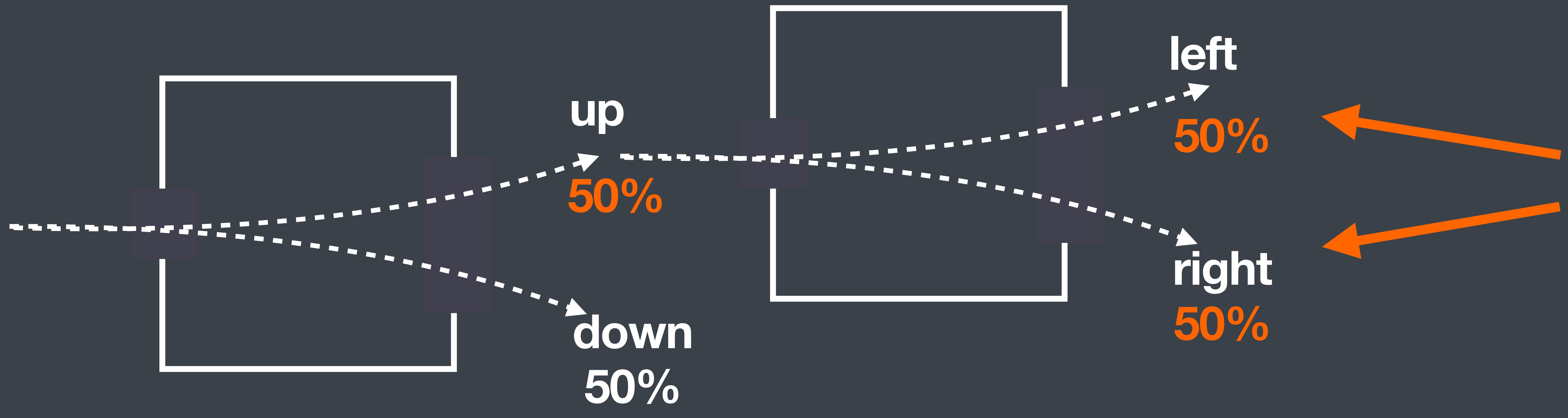
The Stern-Gerlach Experiment



The Stern-Gerlach Experiment

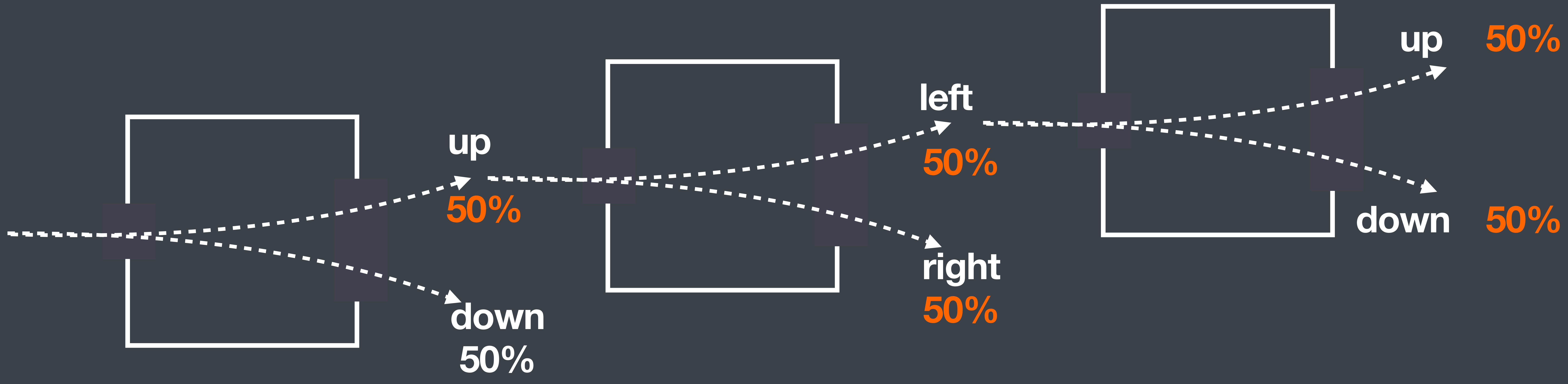


The Stern-Gerlach Experiment



How is that possible?

The Stern-Gerlach Experiment



The Stern-Gerlach Experiment

- When you measure in one dimension, you get either 100% up or 100% down (or left/right)

The Stern-Gerlach Experiment

- When you measure in one dimension, you get either 100% up or 100% down (or left/right)
- You don't really know the result until you actually do the measurement

The Stern-Gerlach Experiment

- When you measure in one dimension, you get either 100% up or 100% down (or left/right)
- You don't really know the result until you actually do the measurement
- Once being measured, you keep measuring the same value when measuring in the same dimension

The Stern-Gerlach Experiment

- When you measure in one dimension, you get either 100% up or 100% down (or left/right)
- You don’t really know the result until you actually do the measurement
- Once being measured, you keep measuring the same value when measuring in the same dimension
- If you measure in a new dimension, the previous measurement falls apart (and re-measuring an already known dimension may yield a different result)

The Stern-Gerlach Experiment

- When you measure in one dimension, you get either 100% up or 100% down (or left/right)
- You don't really know the result until you actually do the measurement
- Once being measured, you keep measuring the same value when measuring in the same dimension
- If you measure in a new dimension, the previous measurement falls apart (and re-measuring an already known dimension may yield a different result)

This feels different from observing a tennis ball
We need a new term to describe it: Superposition

Superposition

You often hear superposition explained as the particle is everything at the same time, or people say that it can be both zero and one at the same time.

It is more a philosophic than a physical discussion: We cannot observe a simular phenomenon with our eyes/hands, so our language is insufficuent to fully describe it.

Superposition means that once measuring, there is a certain probability for each possible outcome.

Superposition

Superposition means that once measuring, there is a certain probability for each possible outcome.

It is like the dice is in superposition until being (thrown and) observed. But would you claim that it is everything at the same time until observed?

(from colinsdictionary.com)

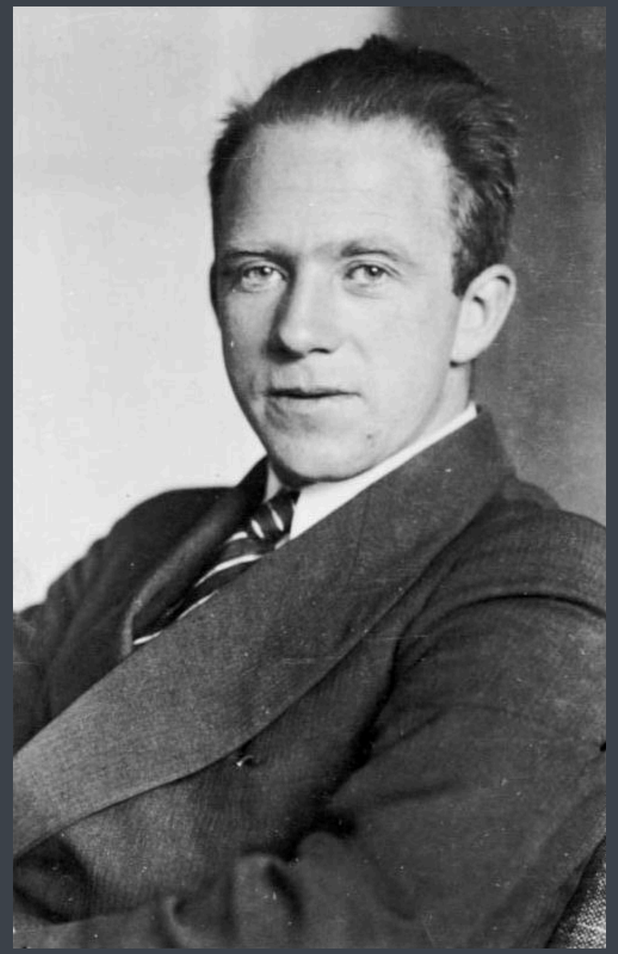
Uncertainty Principle

These observations and theories helped forming Heisenberg's uncertainty principle

(which basically says and proves that you cannot with 100% accuracy know too much of a system's characterics)

And all of this is old news…

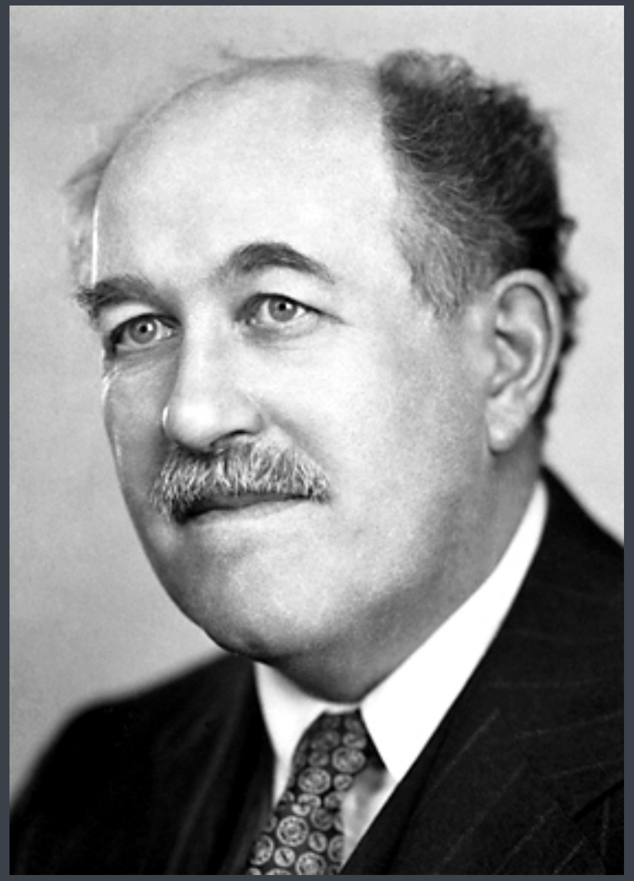
Werner Heisenberg



(from Wikipedia)

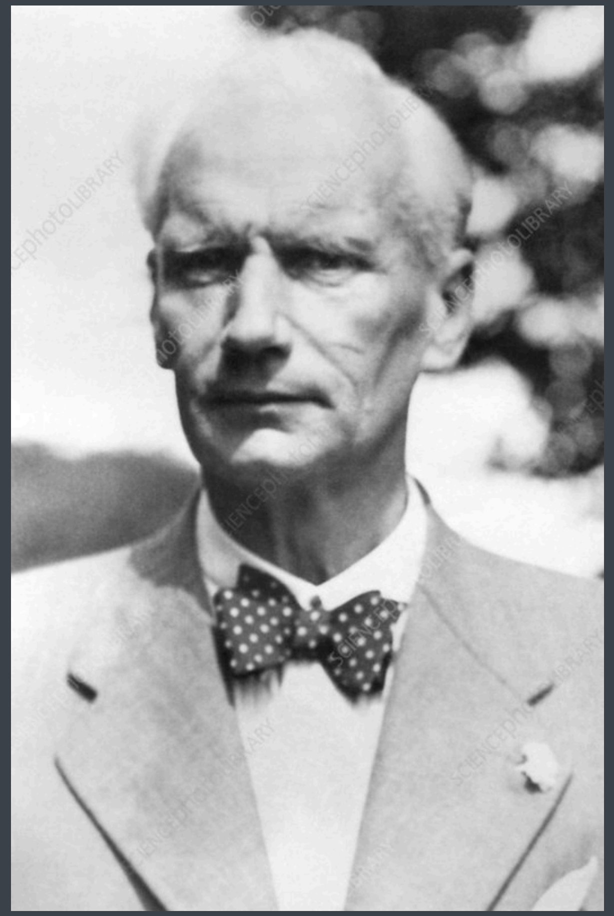
Everything is Old News

Otto Stern



(from Wikipedia)

Walter Gerlach

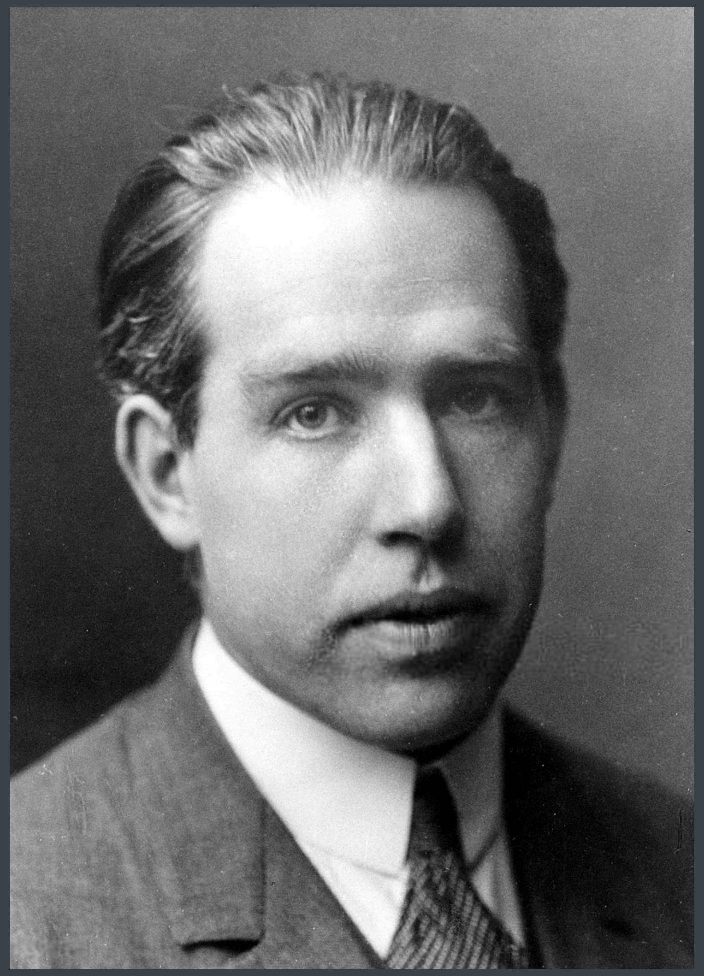


(from sciencephoto.com)

Max Planck

(from Wikipedia)

Niels Bohr



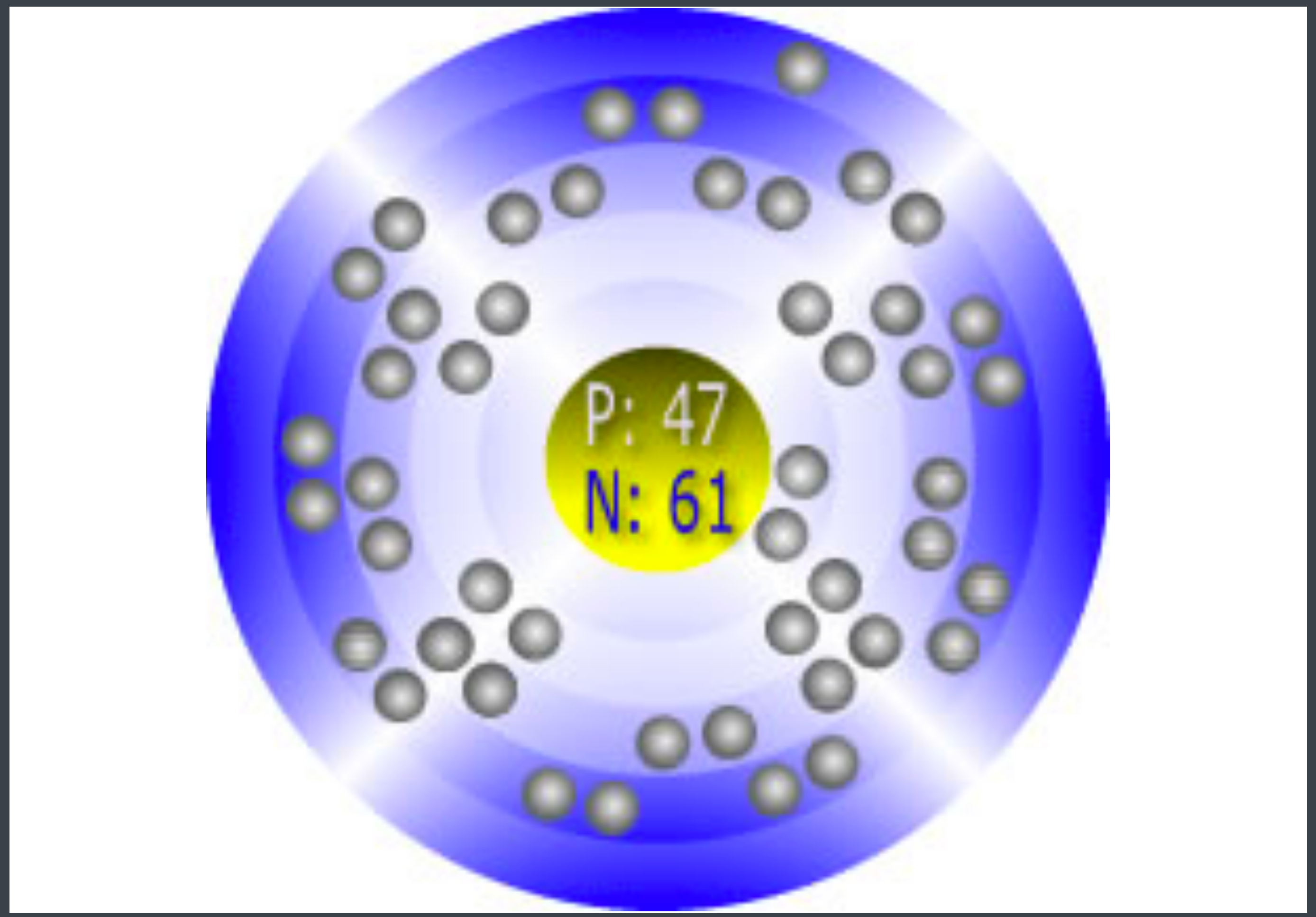
(from Wikipedia)

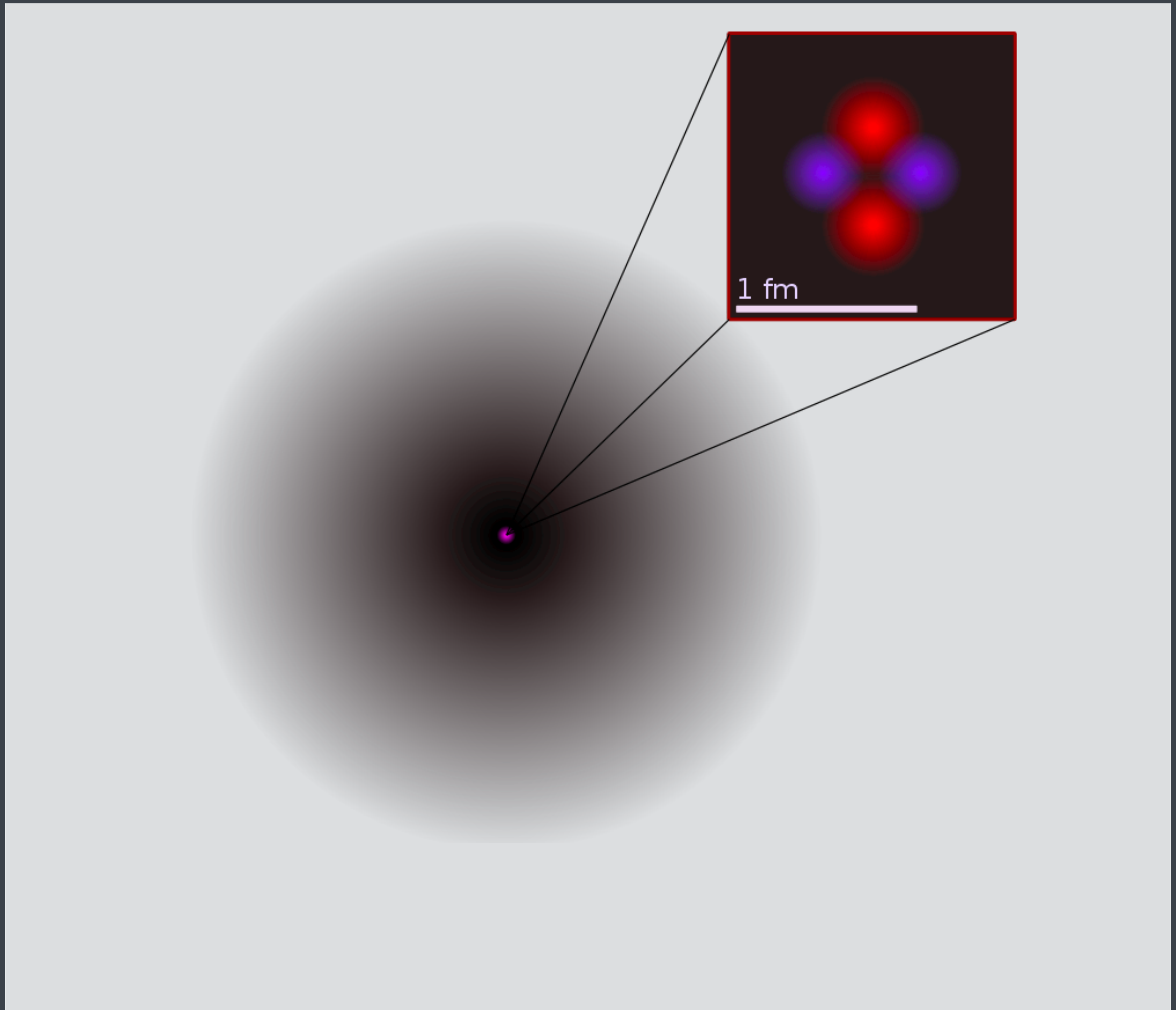
Werner Heisenberg

(from Wikipedia)

(From the 1890s up to the late 1920s)

Wave-Particle Duality

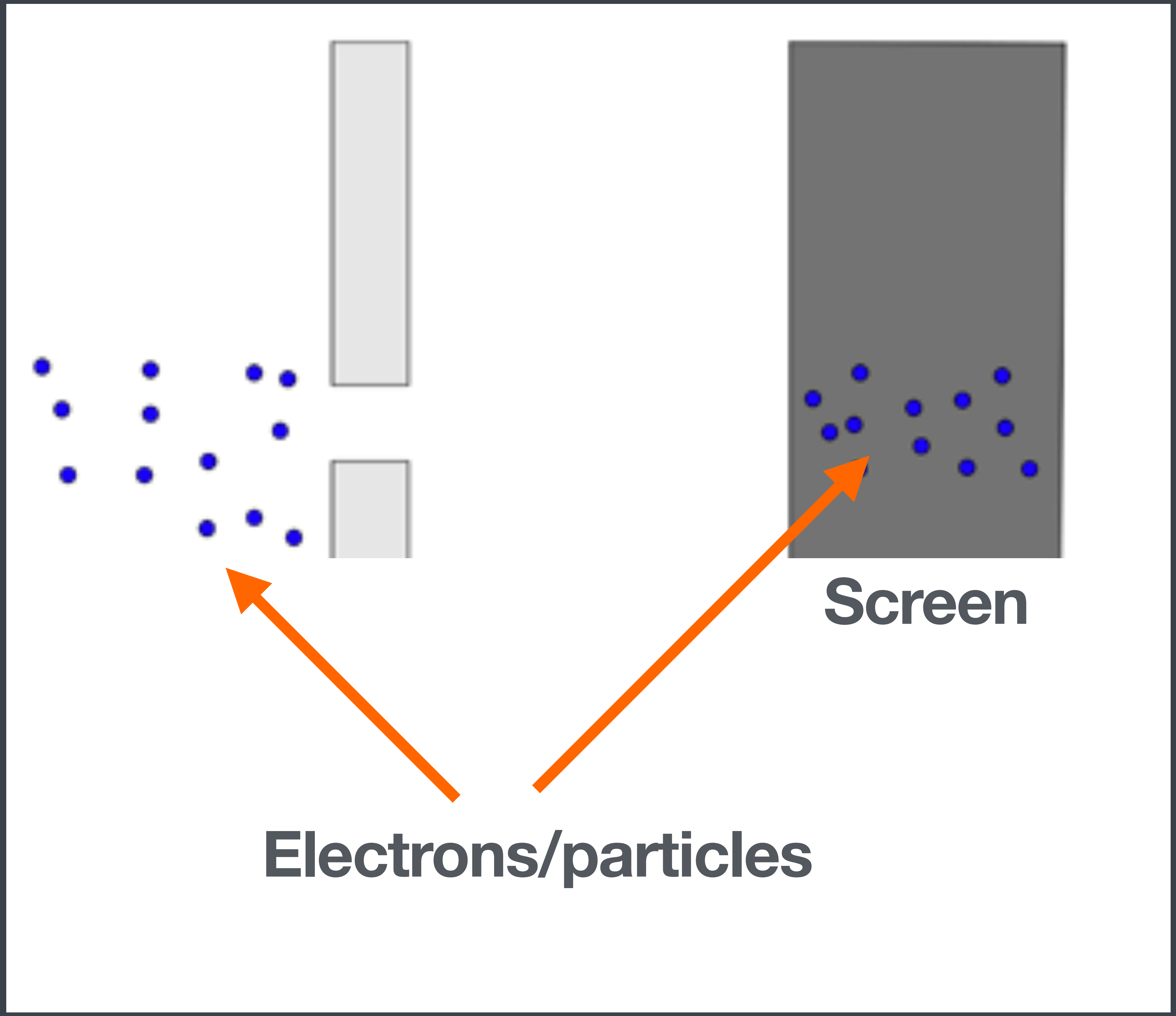




(from wikipedia.org)

Wave-Particle Duality

The 'double slit' experiment

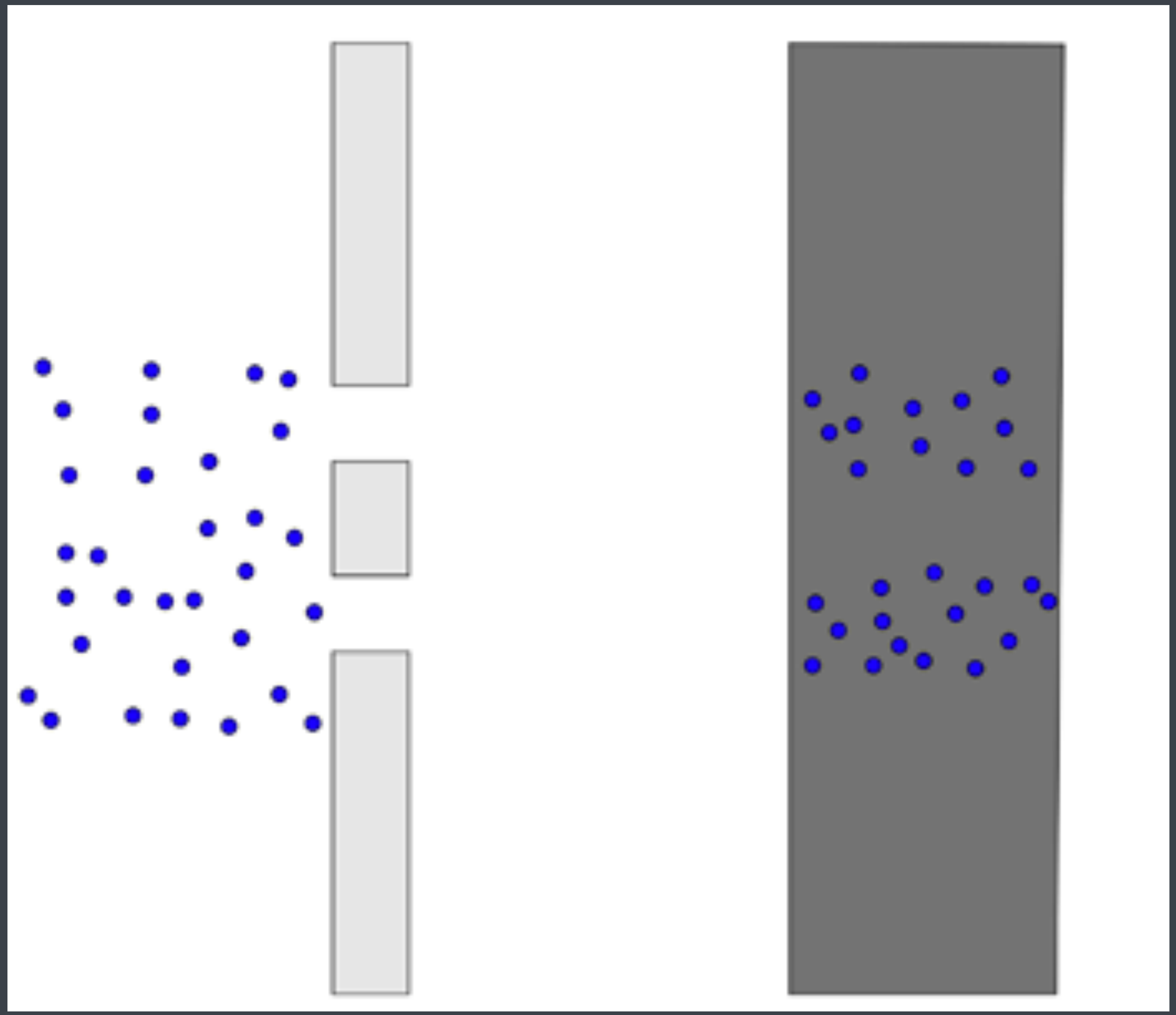


(from plus.math.org)

Wave-Particle Duality

The 'double slit' experiment

Expected result

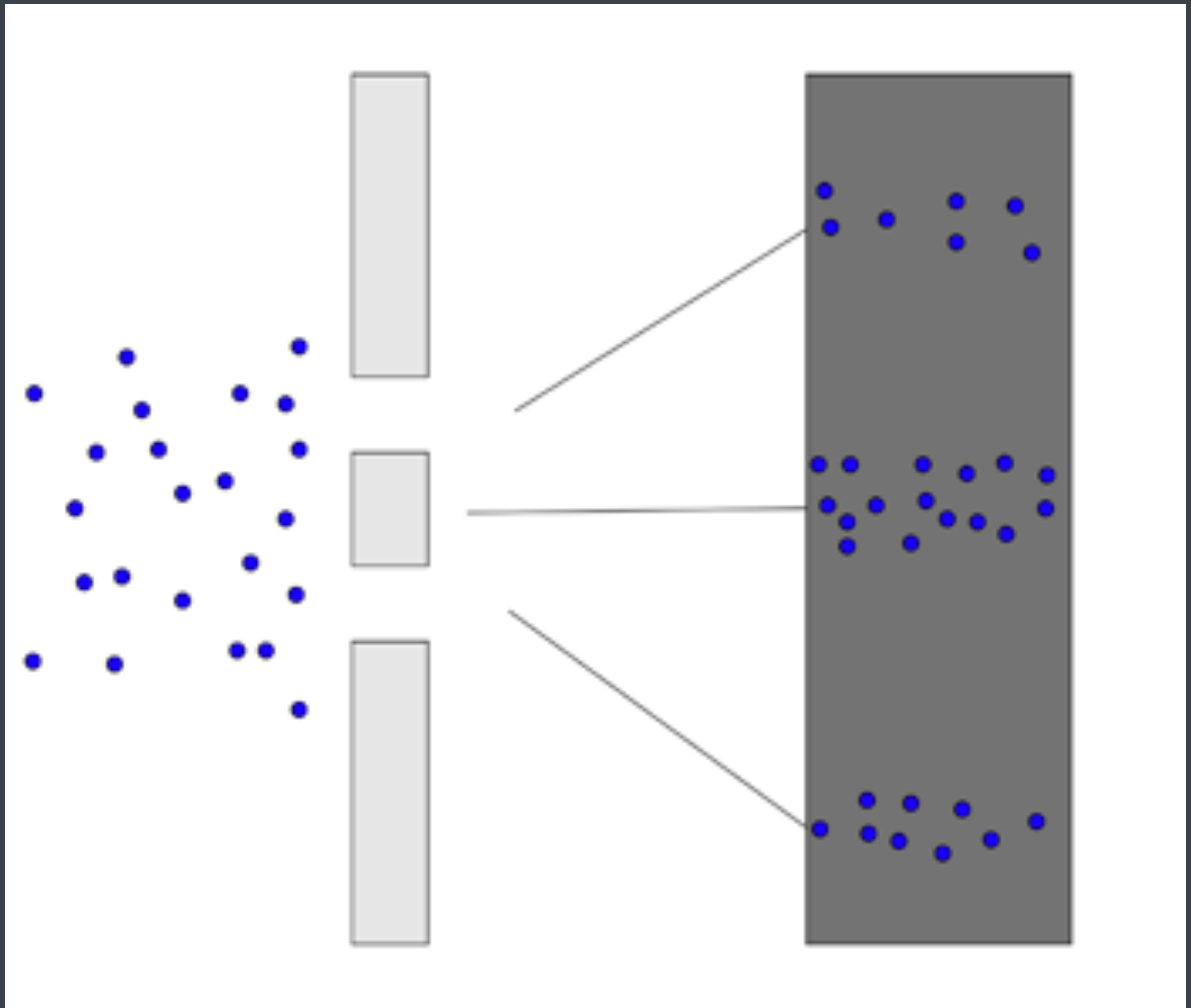


(from plus.math.org)

Wave-Particle Duality

Actual result

The ‘double slit’ experiment

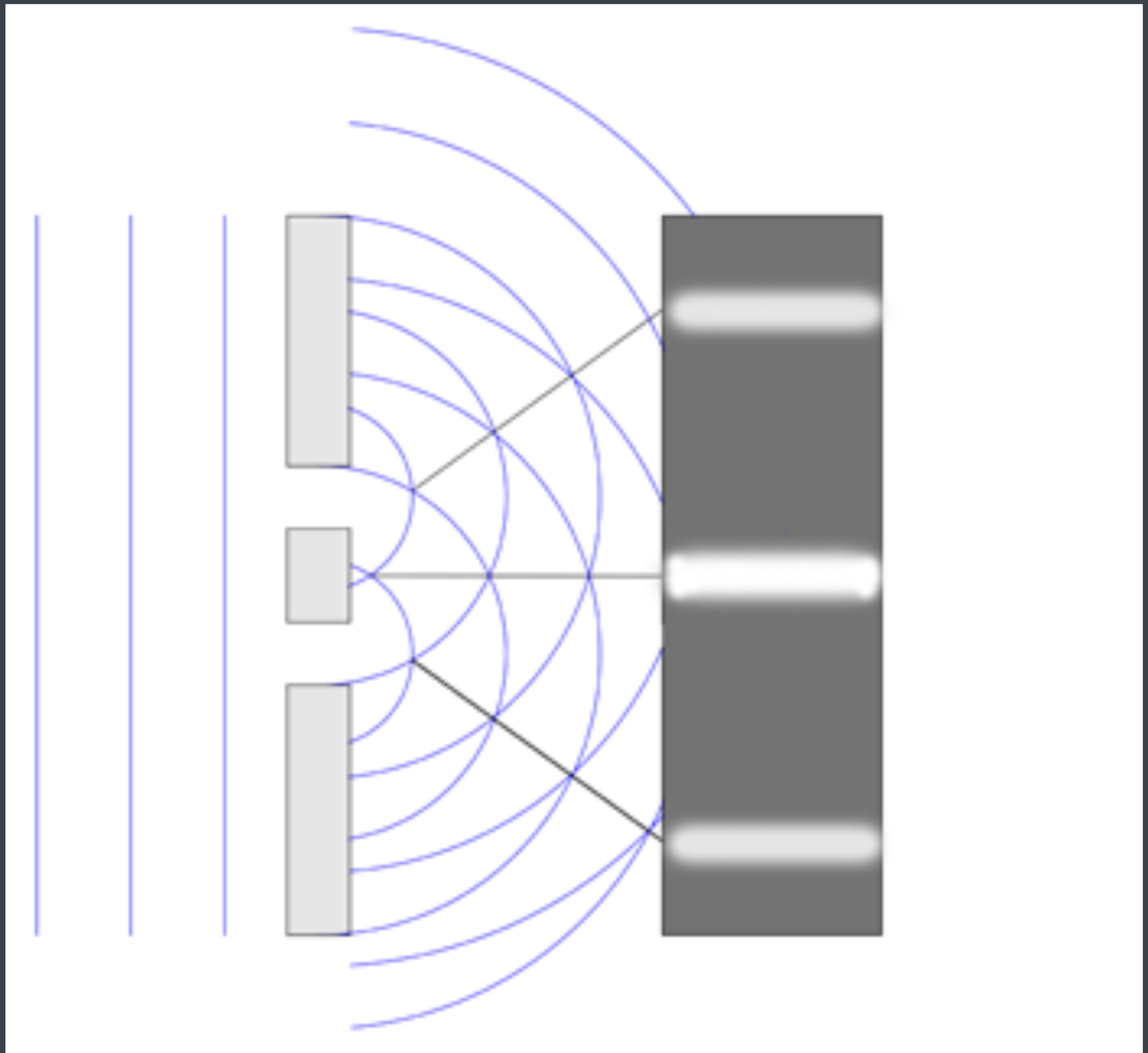


(from plus.math.org)

TRIFORK.
...think software

Wave-Particle Duality

Conclusion:
The particles come through as waves, interfering constructively or desctructively on the other side of the wall

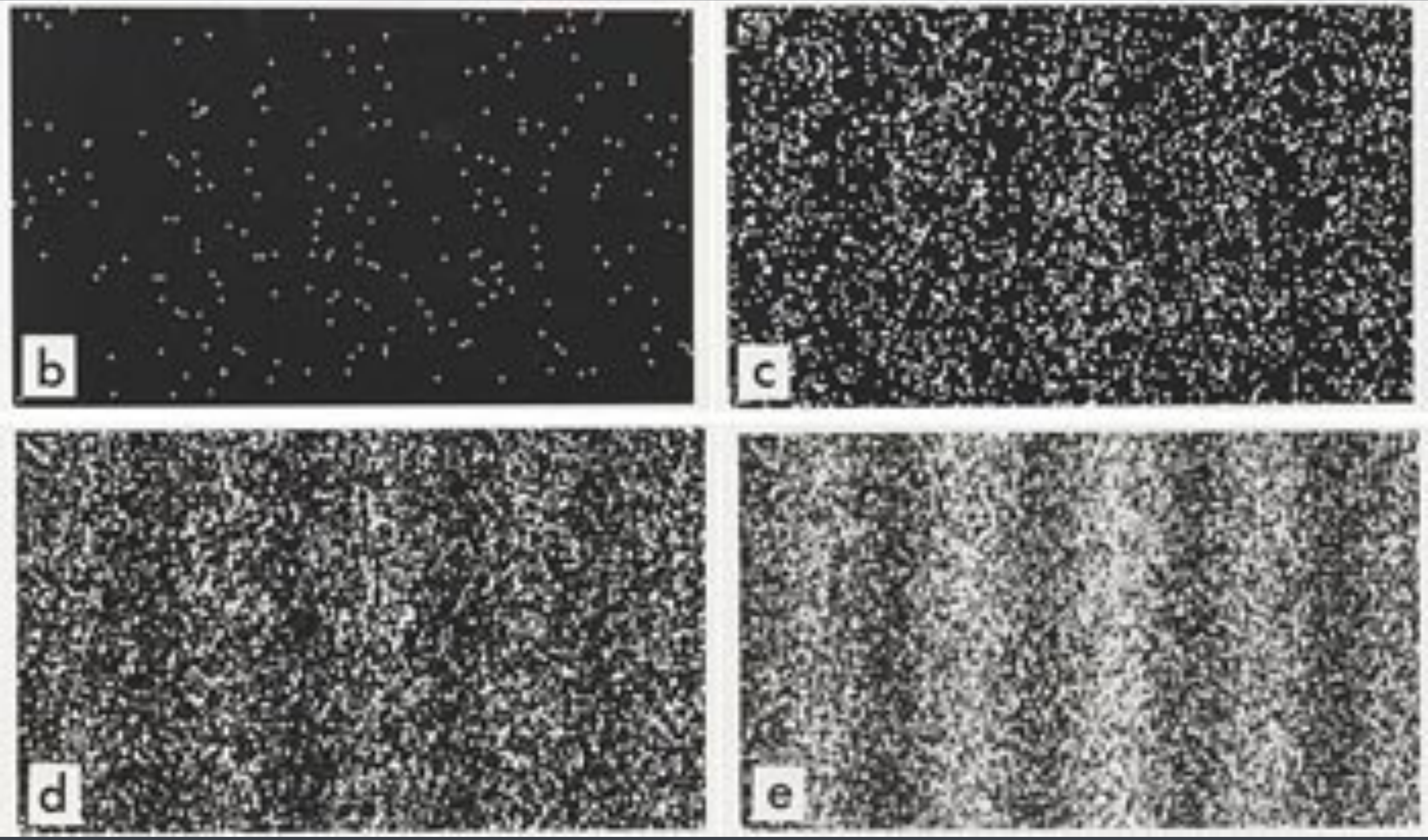


(from plus.math.org)

Wave-Particle Duality

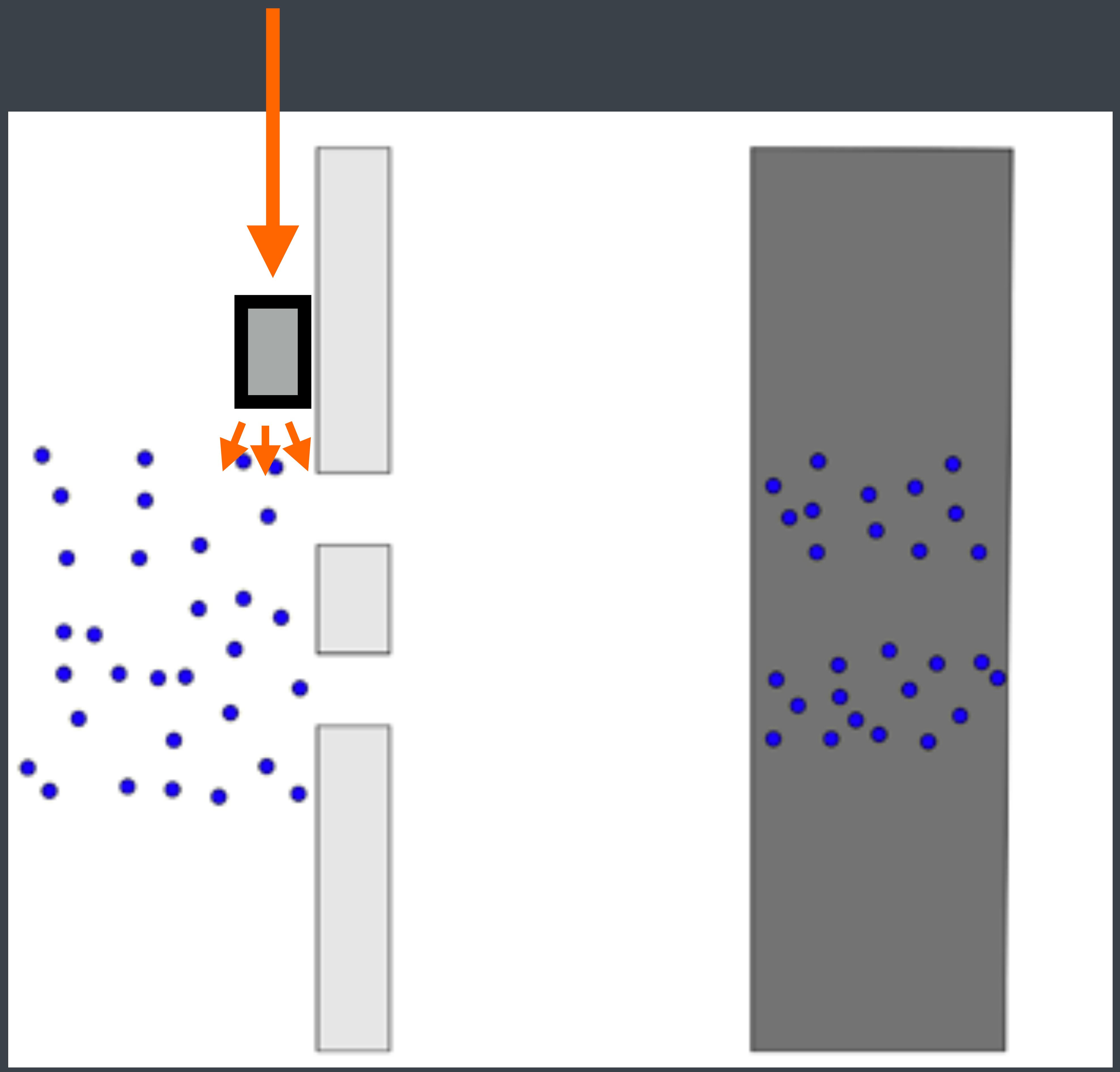
Even shooting the particles through one by one, eventually they end up with the same intereference pattern.

So either each particle flies through both slits, or they somehow interfere on the left side before flying through



(from plus.math.org, originally from Dr. Tonomura and Belsazar, CC BY-SA 3.0))

Wave-Particle Duality



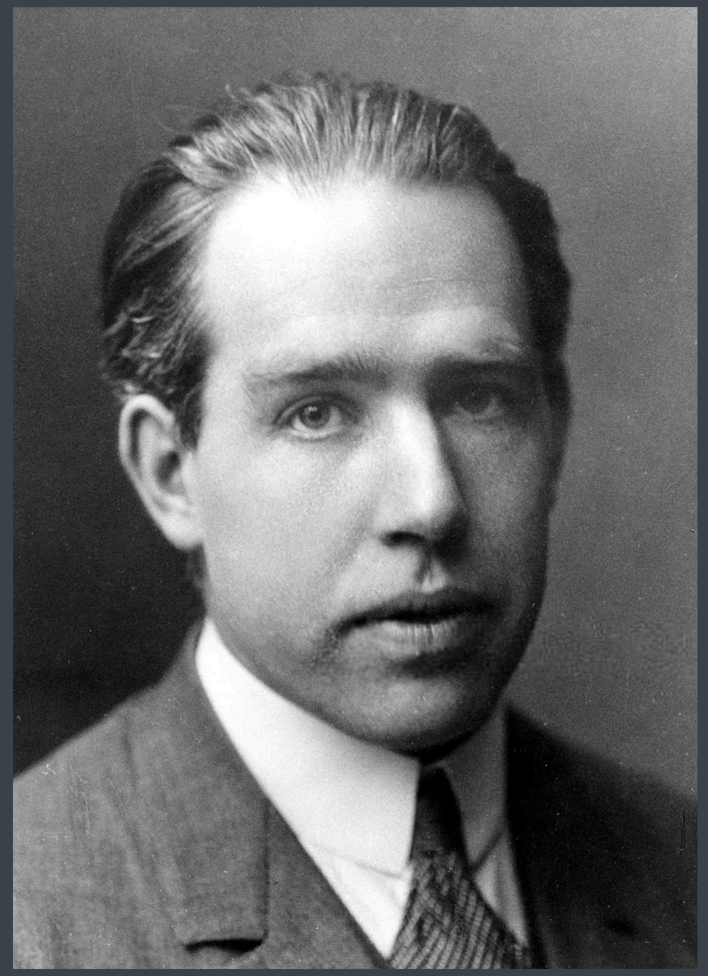
(from plus.math.org)

Wave-Particle Duality

The Copenhagen Interpretation
(As first suggested by Niels Bohr in 1920)

If we decide to measure a particle as a particle, it becomes a particle and stays a particle.
But it seems that the particle is a wave until then.

This becomes important in a moment…

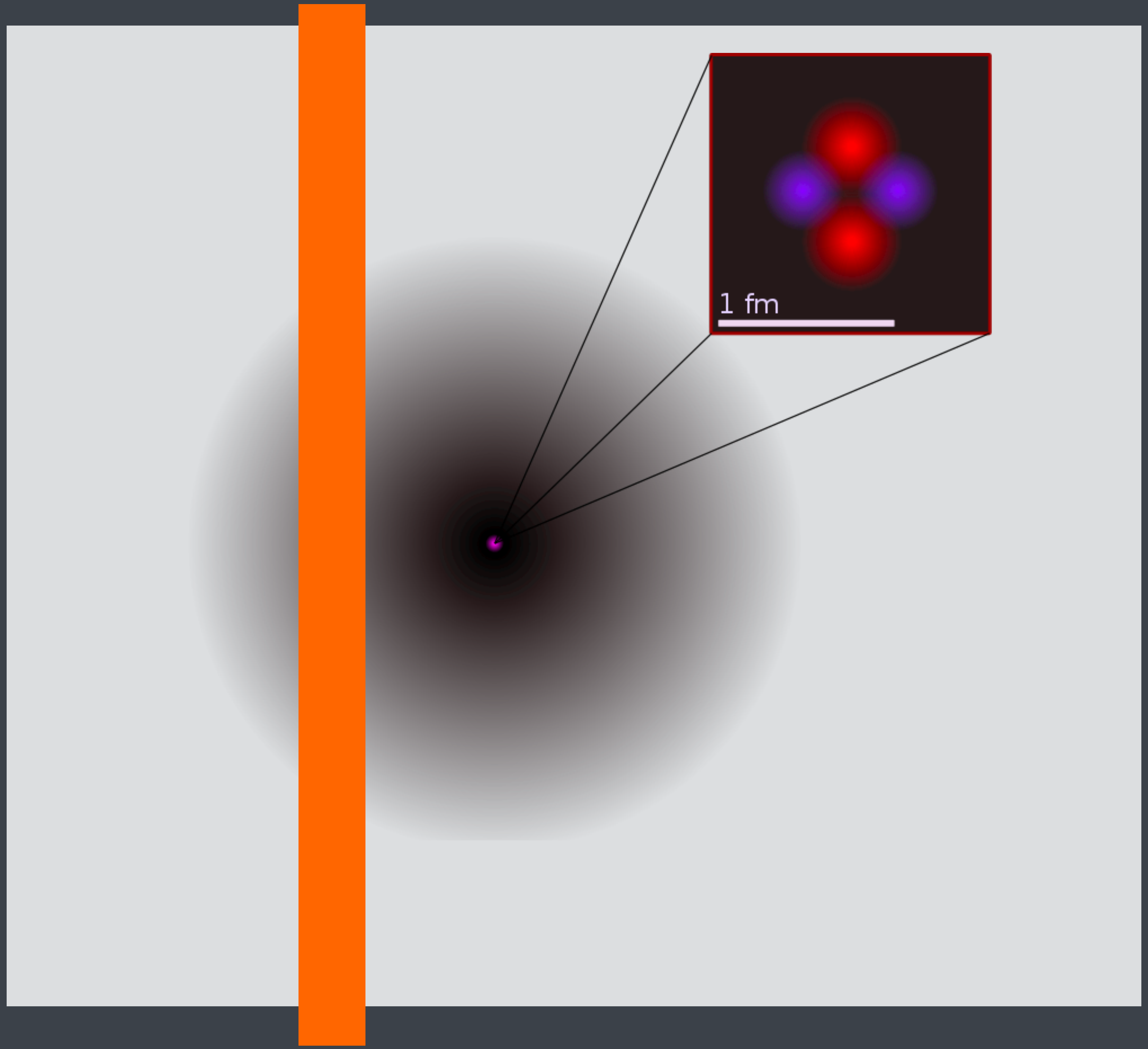


(from wikipedia)

Quantum Tunnelling

We can “feel” the electrons,
measure the energy on the other side of the wall.

This is actually the reason why we cannot keep making the transistors in conventional computer chips smaller: Through quantum tunneling they disturb each other.



Closed wall

TRIFORK.
...think software

Entanglement

Imagine two particles in perfect sync:

Once you measure one of them, you know the outcome of the other one, if you should decide to measure that one too.

Entanglement

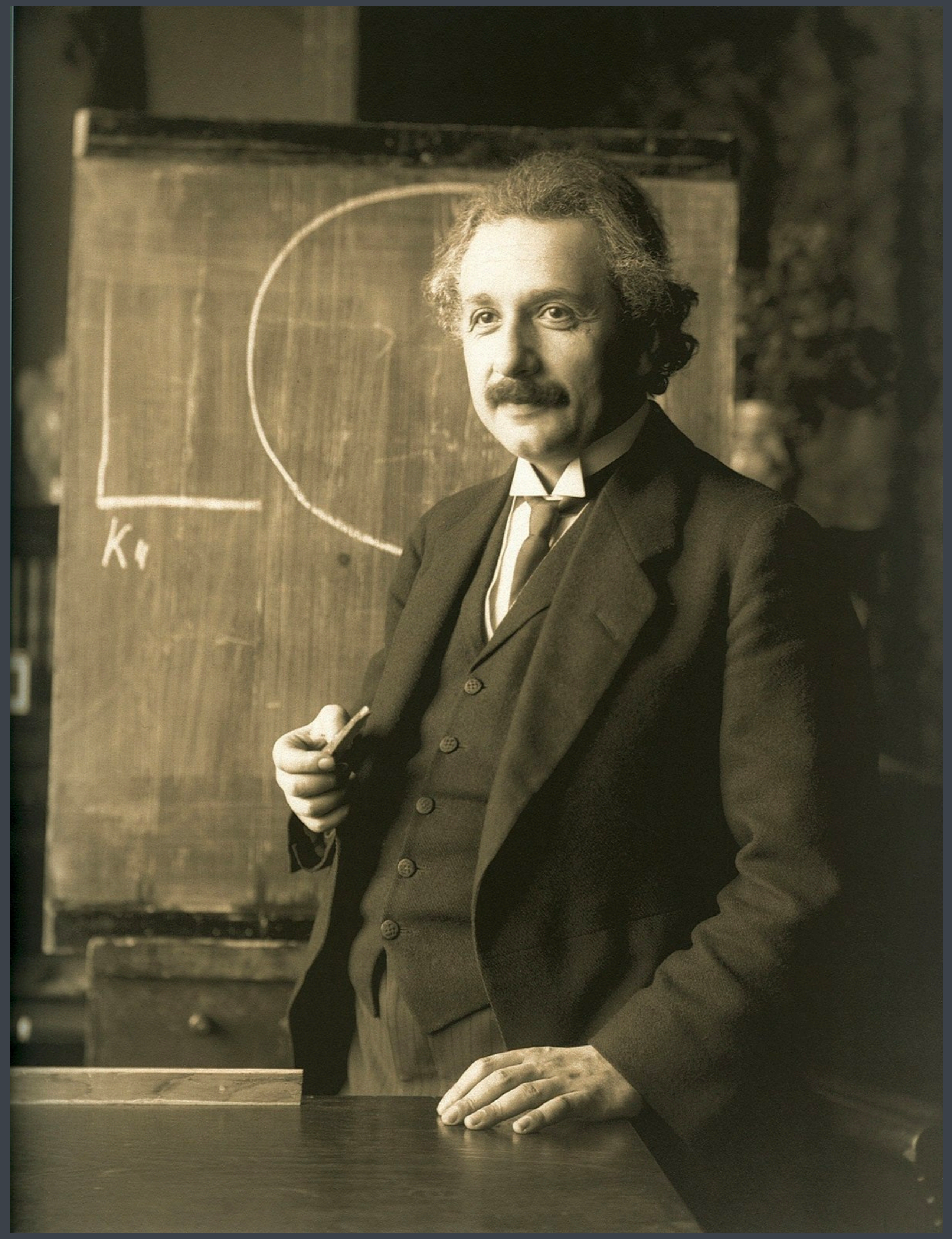
Two electrons, one spinning up, one spinning down

Like one object

Superposition until measurement

Is this in fact time travel?

Albert Einstein



(from wikipedia)

Just to Repeat Myself

Superposition, entanglement, tunnelling are fundamental principles of the universe.
But I cannot logically describe it…

The world I can see and feel formed my language.
We like to see an atom/electron/photon/particle as a flying ball, but that is because we can only relate it to the world we can see and feel.

It is all the same with complex numbers, small particles or big black holes (which actually have zero dimension): We cannot relate it to anything we can see or hold in our hands.
We can only describe it with math.

And we can prove the math through experiments.

Quantum Computing

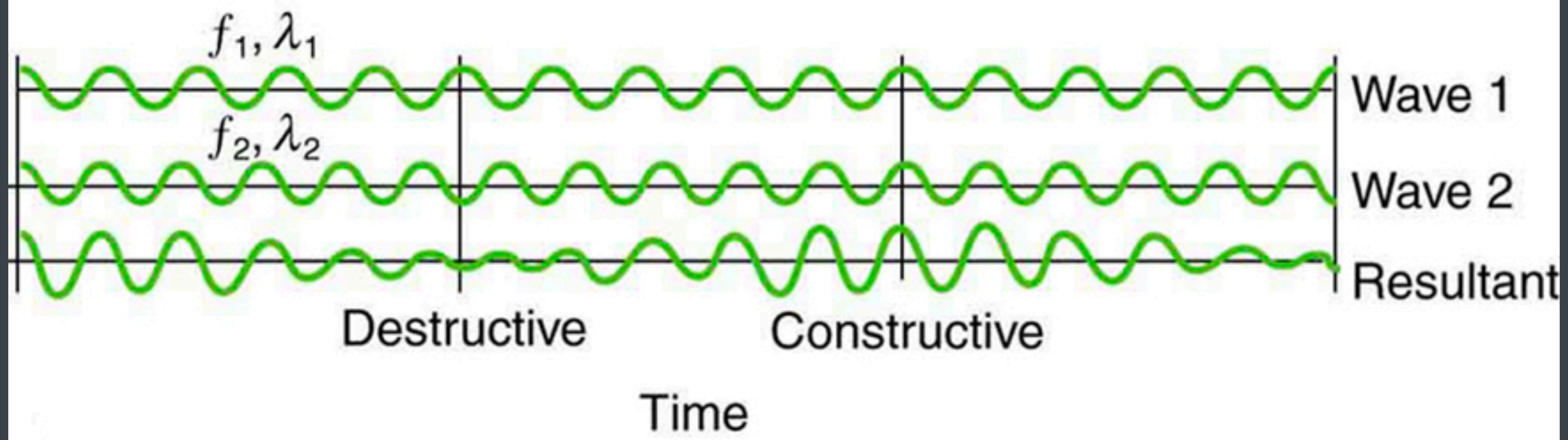
In superposition, there was a 50-50 outcome of the measurement.

What if we could change that to 90-10 or even 99-1 ?

And no one said that we cannot interact with the particles, we are just not allowed to measure them…

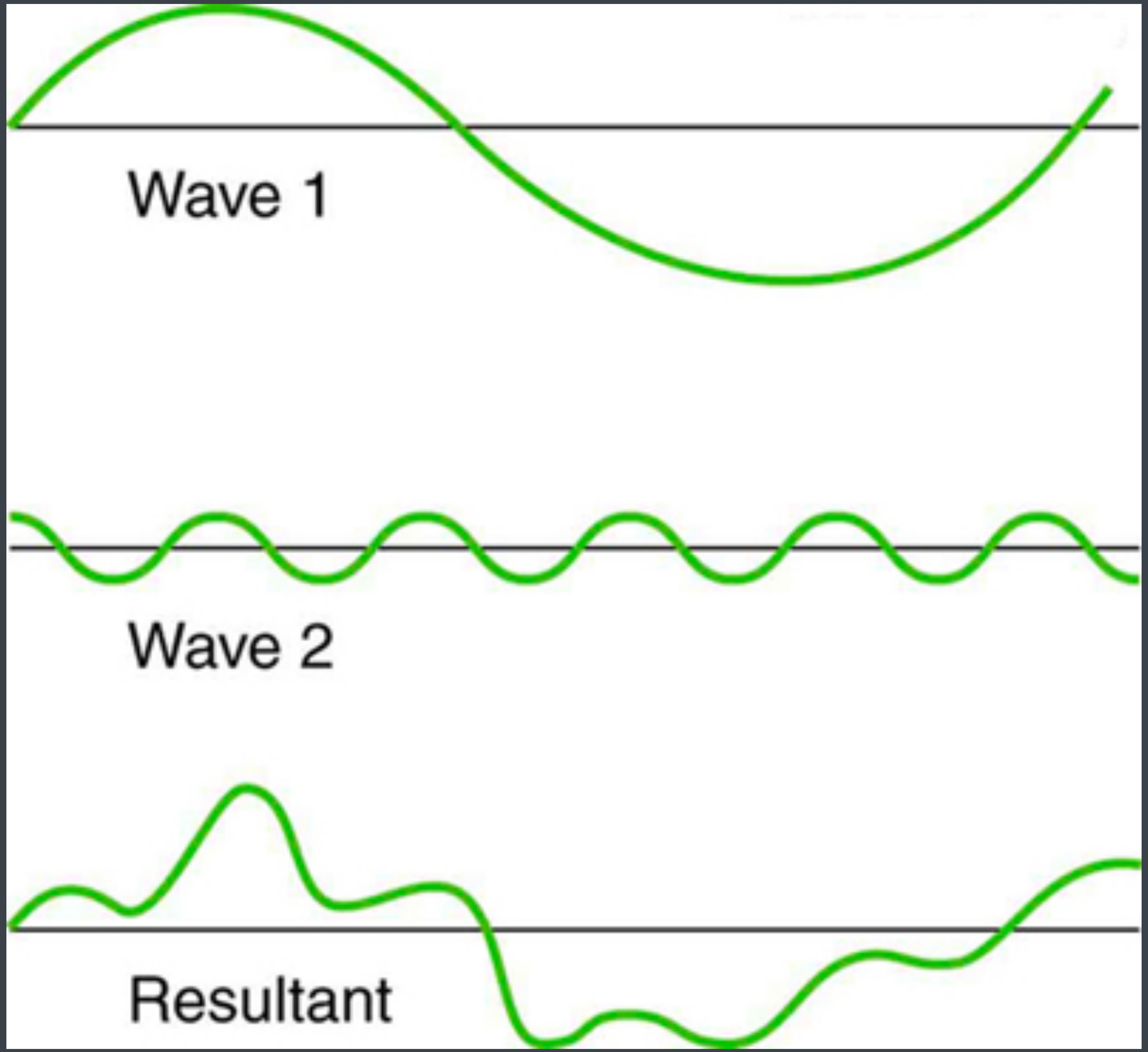
This is weird!

Quantum Computing



What if we could change that to 90-10 or even 99-1 ?

What if the waves given by a suitable combination of particles and entangled particles could cancel out the wrong answers and amplify the correct one?



(from courses.lumenlearning.com)

Quantum Computing

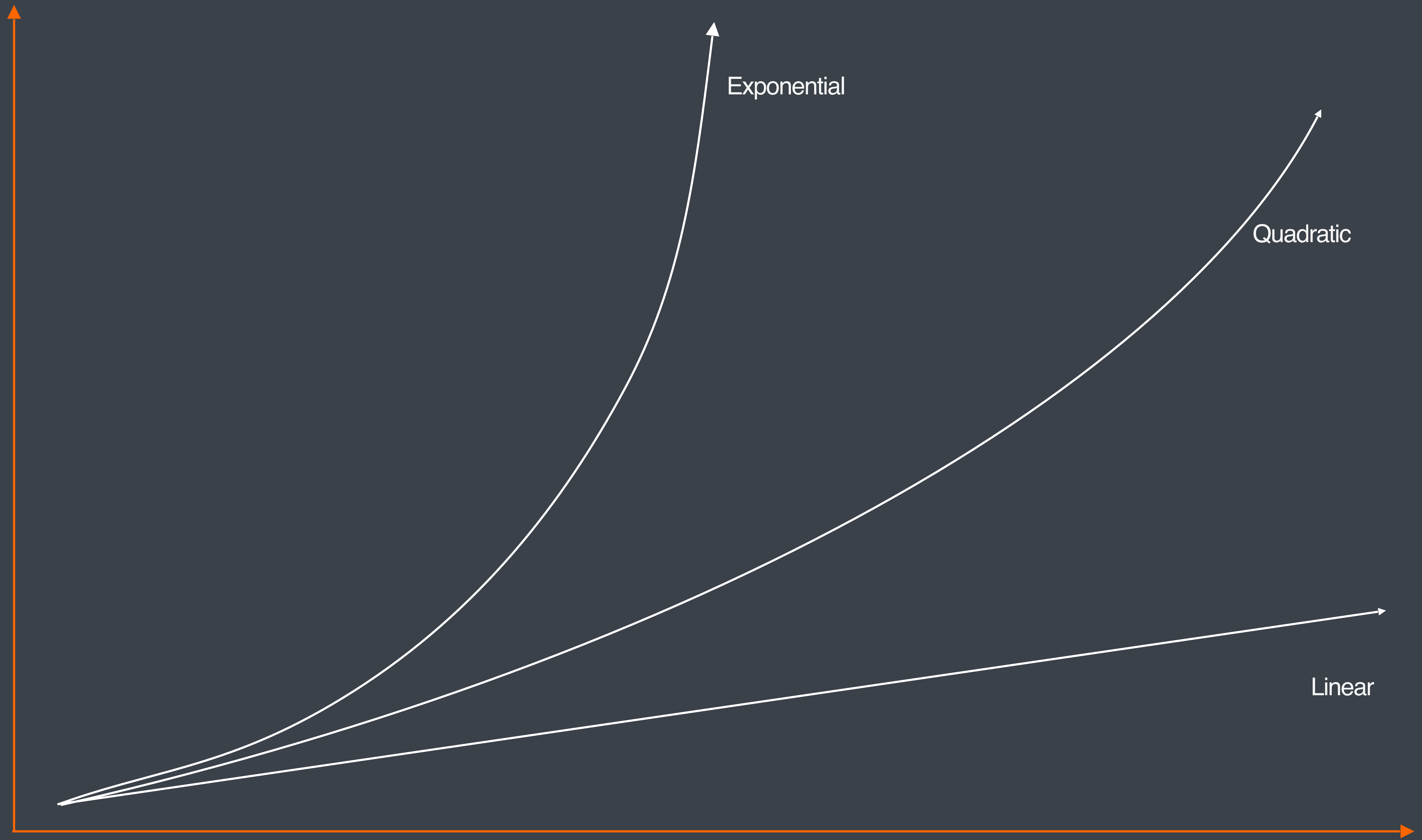
From the early 80s:

There is a certain type of quantum related problems that it does not make sense to simulate on anything else than quantum inspired hardware…

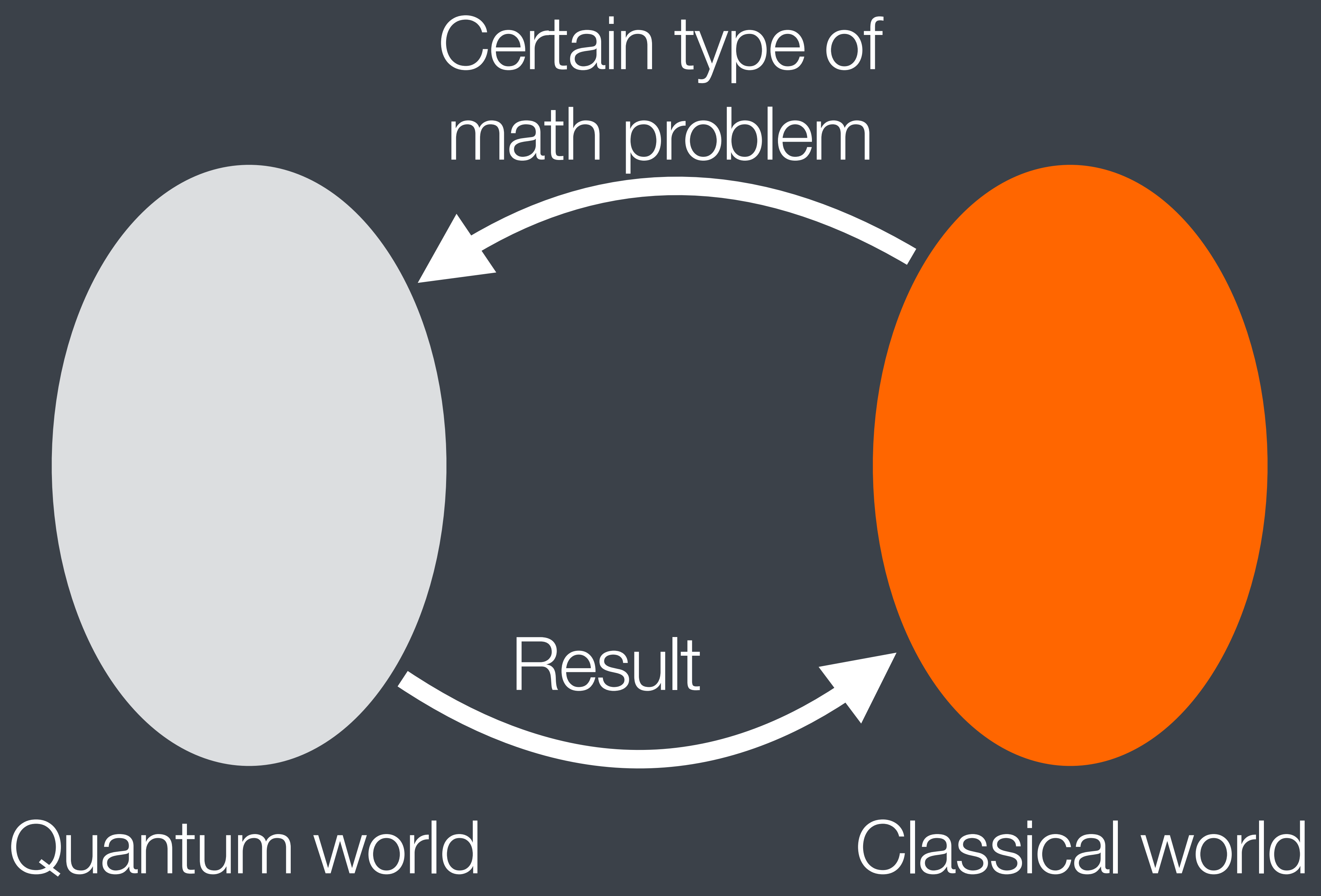
Richard Feynman

(From Wikipedia. Copyright by Tamko Thiel 1984)

Quantum Computing

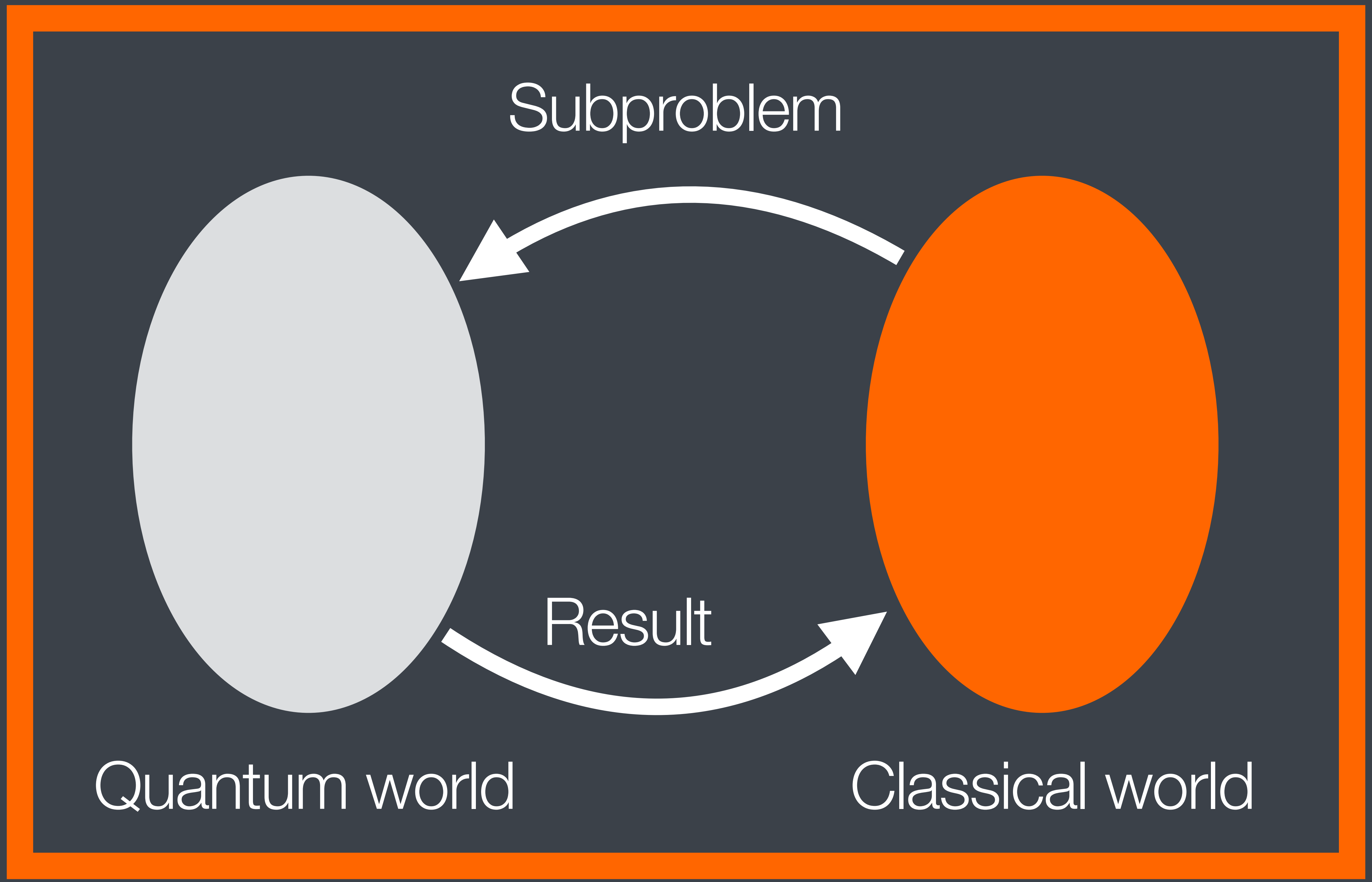


Quantum Computing



It has been proven many times that certain types of math problems can be moved into the quantum space to reduce complexity just like we do when dealing with complex numbers and imaginary dimensions.

Quantum Computing



Hybrid computer

It has been proven many times that certain types of **math** problems can be moved into the quantum space to reduce complexity just like we do when dealing with complex numbers and imaginary dimensions.

QC does not make sense for **IF, THEN, ELSE,** …

Quantum Computers

The basic part is one single unit that shows quantum behaviour (an atom, an electron, a photon, an ion) which we call a ***qubit***

All we need to do is to manipulate the qubit into superposition, manupilate it, entangle it, let it interfere with all the other qubit, let it run long enough and read the results…

Or to put it another way: To line up all qubit for the problem at hand, put the computer to superposition, let it run/stabilize and read out the result

Cryptography

Which two prime numbers made up the number 15 ?

Which two prime numbers made up the number 713 ?
(23 and 31)

What if you multiplied two 300 digit prime numbers?

Cryptography

What if you multiplied two 300 digit prime numbers?

Impossible to solve for human beings

Impossible to solve within resonable time for even the largest battery of the largest super computers

What is resonable time anyway?

Cryptography

Here is how you can break it:

N = p * q

a equals **x MOD N** means that **x/N**, the remainder is **a**

2 * 3 MOD 5 = 1 because **2*3/5** gives a remainder of **1**

Cryptography

Euler taught us something interesting:

3^k **MOD 7** →

3^1 **MOD 7 = 3 MOD 7 = 3**

3^2 **MOD 7 = 9 MOD 7 = 2**

3^3 **MOD 7 = 27 MOD 7 = 6**

3^4 **MOD 7 = 81 MOD 7 = 4**

3^5 **MOD 7 = 243 MOD 7 = 5**

3^6 **MOD 7 = 729 MOD 7 = 1**

3^7 **MOD 7 = 2187 MOD 7 = 3**

3^8 **MOD 7 = 6561 MOD 7 = 2**

3^9 **MOD 7 = 19683 MOD 7 = 6**

And so on…

It repeats forever

TRIFORK.
...think software

Cryptography

Euler taught us something interesting:

3^1 MOD 7 = 3 MOD 7 = 3

3^2 MOD 7 = 9 MOD 7 = 2

3^3 MOD 7 = 27 MOD 7 = 6

3^4 MOD 7 = 81 MOD 7 = 4

3^5 MOD 7 = 243 MOD 7 = 5

3^6 MOD 7 = 729 MOD 7 = 1

3^7 MOD 7 = 2187 MOD 7 = 3

3^8 MOD 7 = 6561 MOD 7 = 2

3^9 MOD 7 = 19683 MOD 7 = 6

And so on…

It repeats forever, and the **last digit in the cycle is always 1**

But only if x (3) and N (7) are relatively prime meaning they share no prime factors

IMPORTANT!

TRIFORK.
…think software

Cryptography

Euler taught us something interesting:

$\mathbf{x^1}$ **MOD N**

$\mathbf{x^2}$ **MOD N**

$\mathbf{x^3}$ **MOD N**

$\mathbf{x^4}$ **MOD N**

$\mathbf{x^5}$ **MOD N**

And so on…

If **x** and **N** are relatively prime, they will always show this behaviour: The pattern repeats with a certain period, and the last number within the sequence is always 1

So from the previous example of **3 MOD 7**, the **period** is **6**

Cryptography

Euler taught us something interesting:

x^1 **MOD N**

x^2 **MOD N**

x^3 **MOD N**

x^4 **MOD N**

x^5 **MOD N**

And so on…

Let **r** be the period of **x MOD N**

It turns out that x^r **MOD N = 1 MOD N**

Cryptography

Euler taught us something interesting:

Let **r** be the period of **x MOD N**

It turns out that **r** is the smallest number such that $\mathbf{x^r}$ **MOD N** is the same as **1 MOD N**

From before:

3^1 **MOD 7 = 3 MOD 7 = 3**

3^2 **MOD 7 = 9 MOD 7 = 2**

3^3 **MOD 7 = 27 MOD 7 = 6**

3^4 **MOD 7 = 81 MOD 7 = 4**

3^5 **MOD 7 = 243 MOD 7 = 5**

$\boxed{3^6 \text{ MOD } 7 = 729 \text{ MOD } 7 = 1}$

3^7 **MOD 7 = 2187 MOD 7 = 3**

3^8 **MOD 7 = 6561 MOD 7 = 2**

3^9 **MOD 7 = 19683 MOD 7 = 6**

Cryptography

N = p * q, let's find **p** and **q**:

Step 1: Pick any number, **a**, smaller than **N**. Make sure **a** and **N** are relatively prime

That is easy, ***Euclid*** taught us to compute the *greatest common divisor*, and if it happens to be 1, we're good to go

So if **GCD(a,N) = 1**, move on

If they happen to share a common divisor > 1, it must be either **p** or **q**, and you're already done!

Cryptography

N = p * q, let's find **p** and **q**:

Step 1: Pick any number, **a**, smaller than **N**. Make sure **a** and **N** are relatively prime

Step 2: Compute **r** = the period of **a MOD N**

As we will see later, **r** must be even. If not, pick another **a** and retry.

We also need to ensure that $\mathbf{a^{r/2}}$ **MOD N** is not the same as **0 MOD N**

Step 3: From before we know that $\mathbf{a^{r}}$ **MOD N** is the same as **1 MOD N**

Which means that $\mathbf{a^{r} - 1}$ **MOD N** is the same as **0 MOD N**

Meaning that $\mathbf{a^{r} - 1 = k * N}$ - there must be some factor **k**, fulfilling this

So $\mathbf{a^{r} - 1 = k * p * q}$

Cryptography

Step 3: From before we know that a^r **MOD N** is the same as **1 MOD N**

Which means that $a^r - 1$ **MOD N** is the same as 0 **MOD N**

Meaning that $a^r - 1 = k * N$ - there must be some factor k, fulfilling this

So $a^r - 1 = k * p * q$

From back in school we know that $(x - y)(x + y) = x^2 - y^2$

So we can rewrite the above to $(a^{r/2} - 1)(a^{r/2} + 1) = k * p * q$

Cryptography

Step 4: Now we know that $\mathbf{(a^{r/2} - 1)(a^{r/2} + 1) = k * p * q}$

This means that **p** must divide one of the factors on the left side and **q** must divide one of the factors on the left side.

We assumed that $\mathbf{a^{r/2} + 1}$ **MOD N** is not congruent to **0 MOD N** so it cannot be divisible by **N**

We know that $\mathbf{a^{r}}$ **MOD N** is the same as **1 MOD N**

We also know that **r** is the smallest number so that $\mathbf{a^{r}}$ **MOD N** is the same as **1 MOD N**

So this means that $\mathbf{a^{r/2} -1}$ **MOD N** cannot be congruent to **0 MOD N**

All of this means that $\mathbf{(a^{r/2} - 1)}$ and $\mathbf{(a^{r/2} + 1)}$ are divisible by **p** and **q** respectively, but neither of them divide **N**

Conclusion: **p** must be $\mathbf{GCD(a^{r/2} -1, N)}$ and **q** must be $\mathbf{GCD(a^{r/2}+1,N)}$

TRIFORK.
...think software

Cryptography

Let's try to find the two prime factors of the previous example: **N = 713 = 23 * 31**

Step 1 and 2: Pick any number, **a**, smaller than **713** and compute the period of **a MOD 713**

I choose **a = 12**, and It gives me the period **r = 330**

r is even, that is good

So $(12^{330/2} - 1)(12^{330/2} + 1) = k * 23 * 31$

So show that $GCD(12^{330/2} -1,713) = 23$ **(or 31)** and that $GCD(12^{330/2} +1,713) = 31$ **(or 23)**

But….

TRIFORK.
…think software

Cryptography

Let's try to find the two prime factors of the previous example: **N = 713 = 23 * 31**

$\mathbf{12^{165}}$ …overflow, not a number, error…

I need bigger hardware…

(from de.wikipedia.org)

Cryptography

Let's try another example: **N = 7 * 13 = 91**

I choose **a = 6**, and It gives me the period **r = 12**

So $(6^6 - 1)(6^6 + 1) = k * 7 * 13$

63 * 65 = k * 91

GCD(63,91) = 7, GCD(65,91) = 13

TRIFORK.
...think software

Cryptography

Even working with **N = 713** went beyond my Python script on my laptop

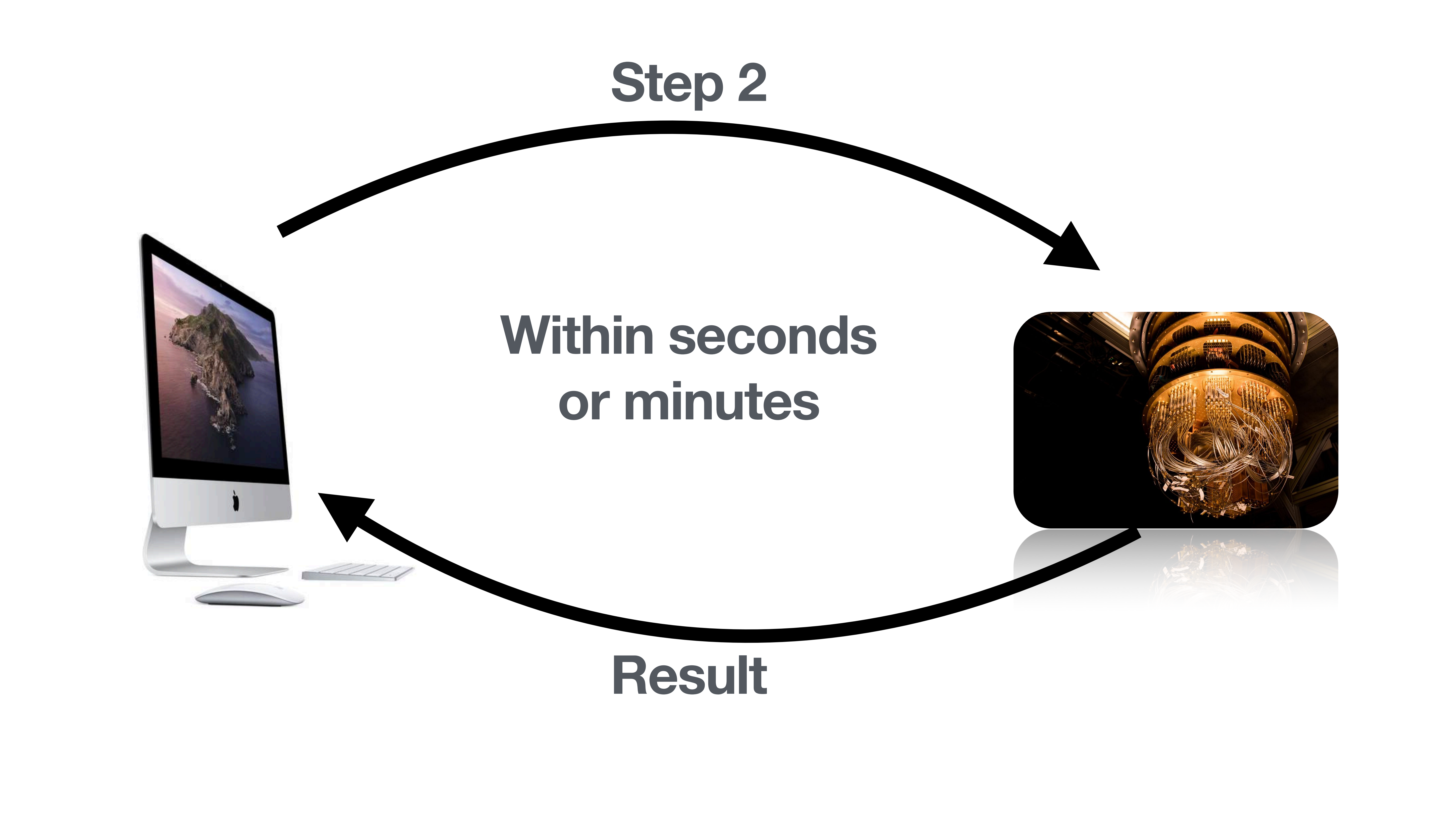
But it is actually not even the most demanding step…step 2 is:

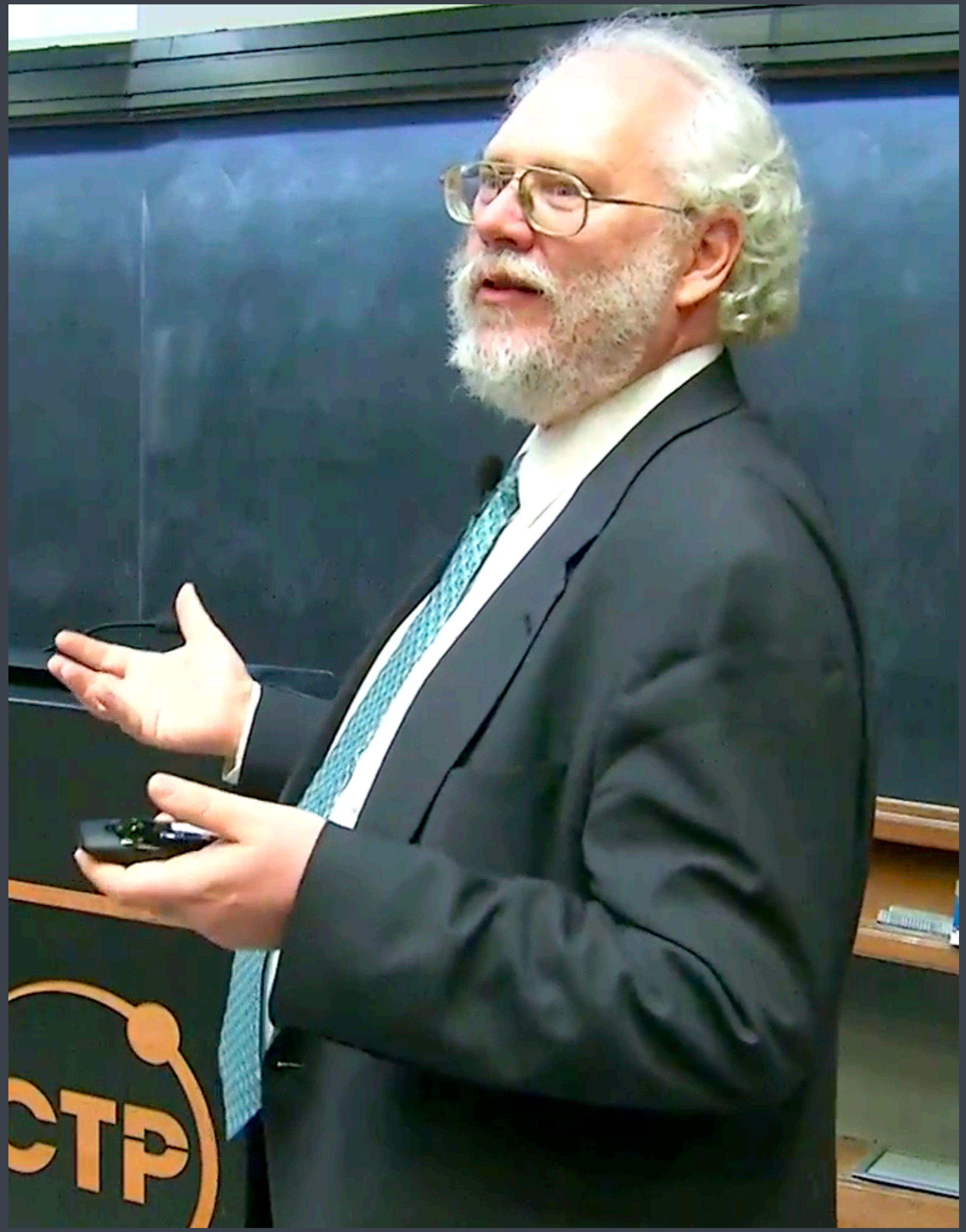
Step 2: Compute **r** = the period of **a MOD N**

Fro real usage, it would take millions of years on even the most extreme bad ass hardware!

Quantum Computing - Encryption

Shor's algorithm (1994)



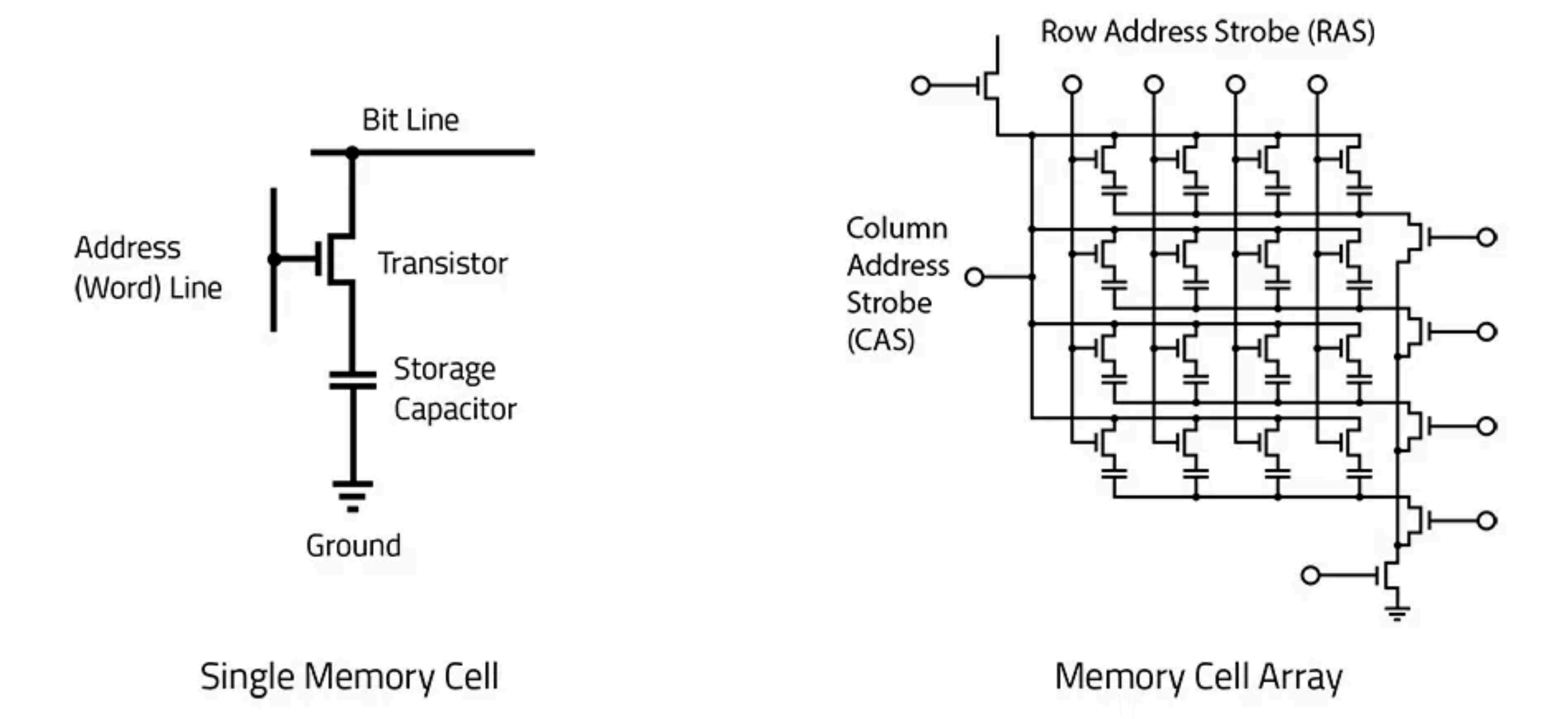


(from Wikipedia)

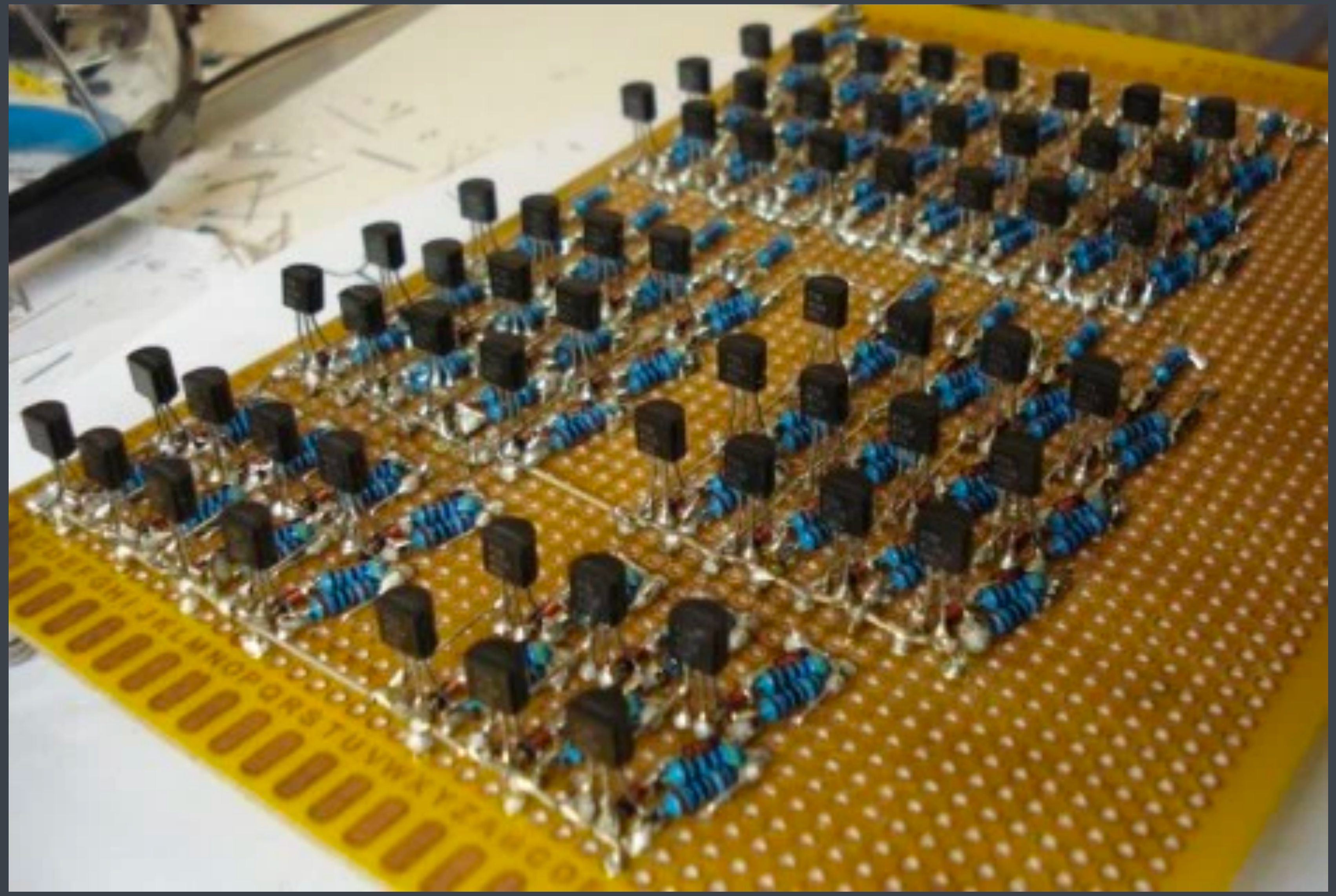
Use QC to find the period…

Before We Move On

(from bcs.org)



(from semiengineering.com)



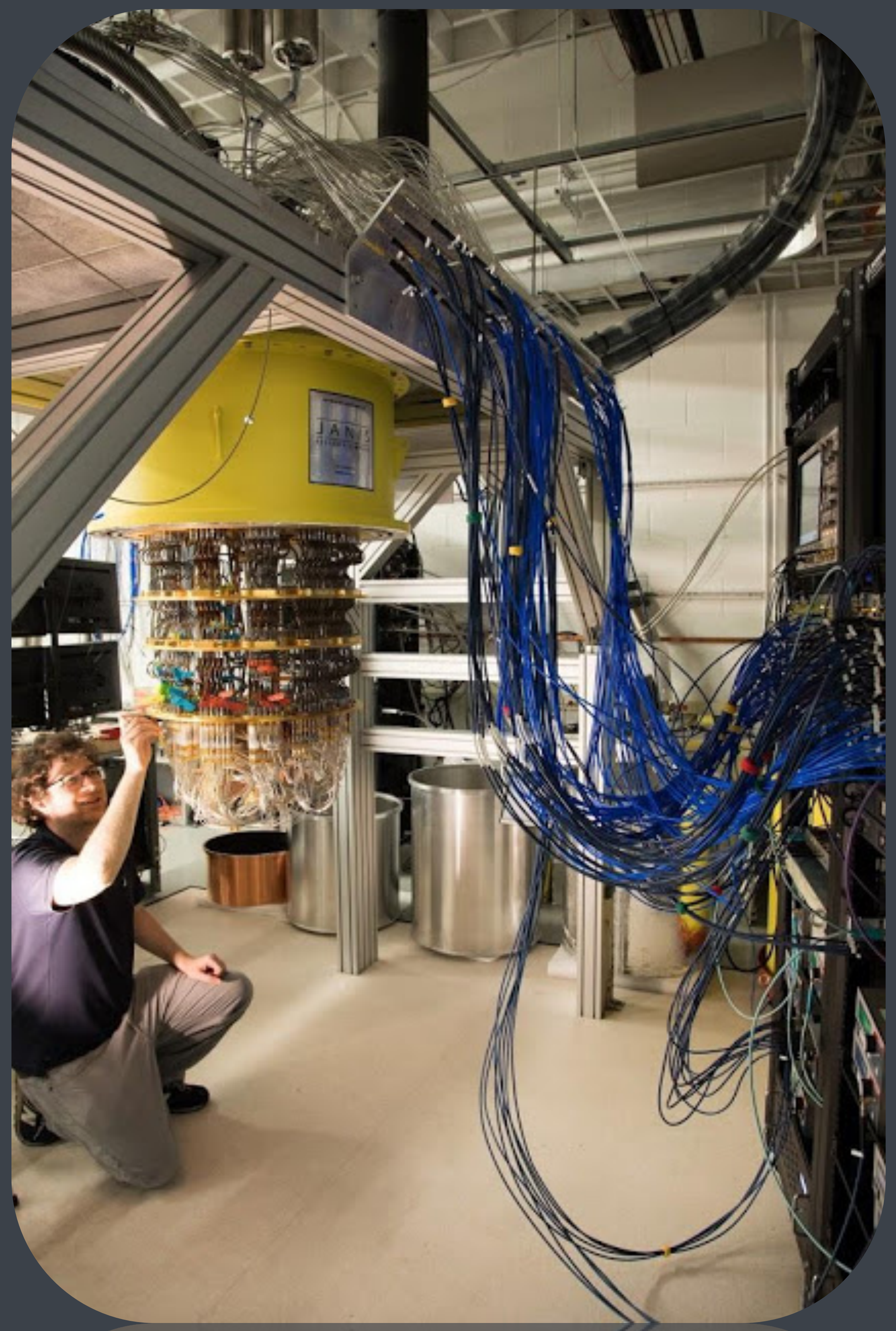
(from hackaday.com)

Quantum Computers

IBM, Google, Xanadu, Rigetti, Honeywell, and many more

Curent state of the art: 50-70 qubits
-> for Shor's algorithm we need close to 6000

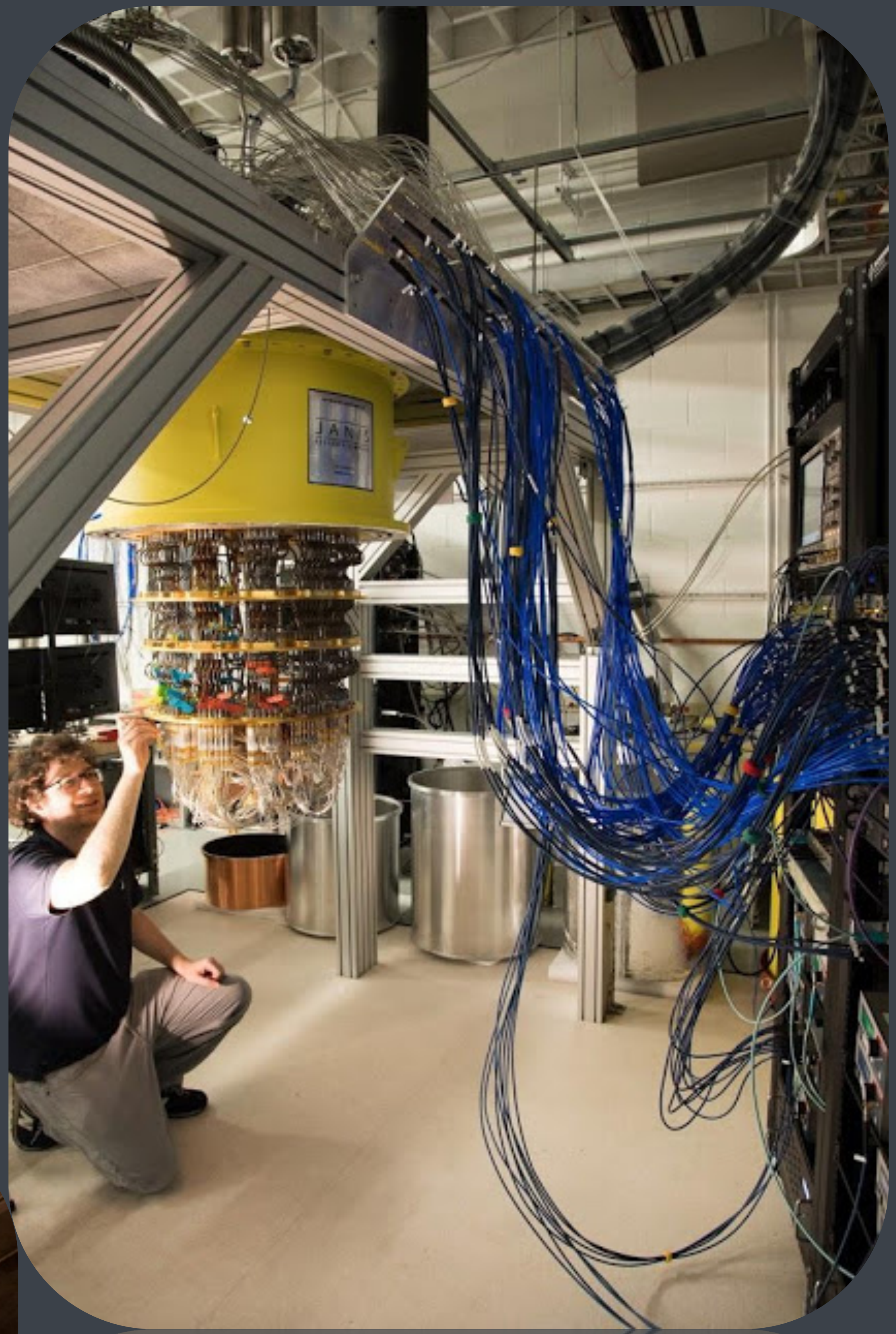
But do they work?



Quantum Computers

- Noise
- Tunnelling
- Decoherence time

For current state of the art we need closer to 1 mill qubits to error correct and run Shor's algorithm

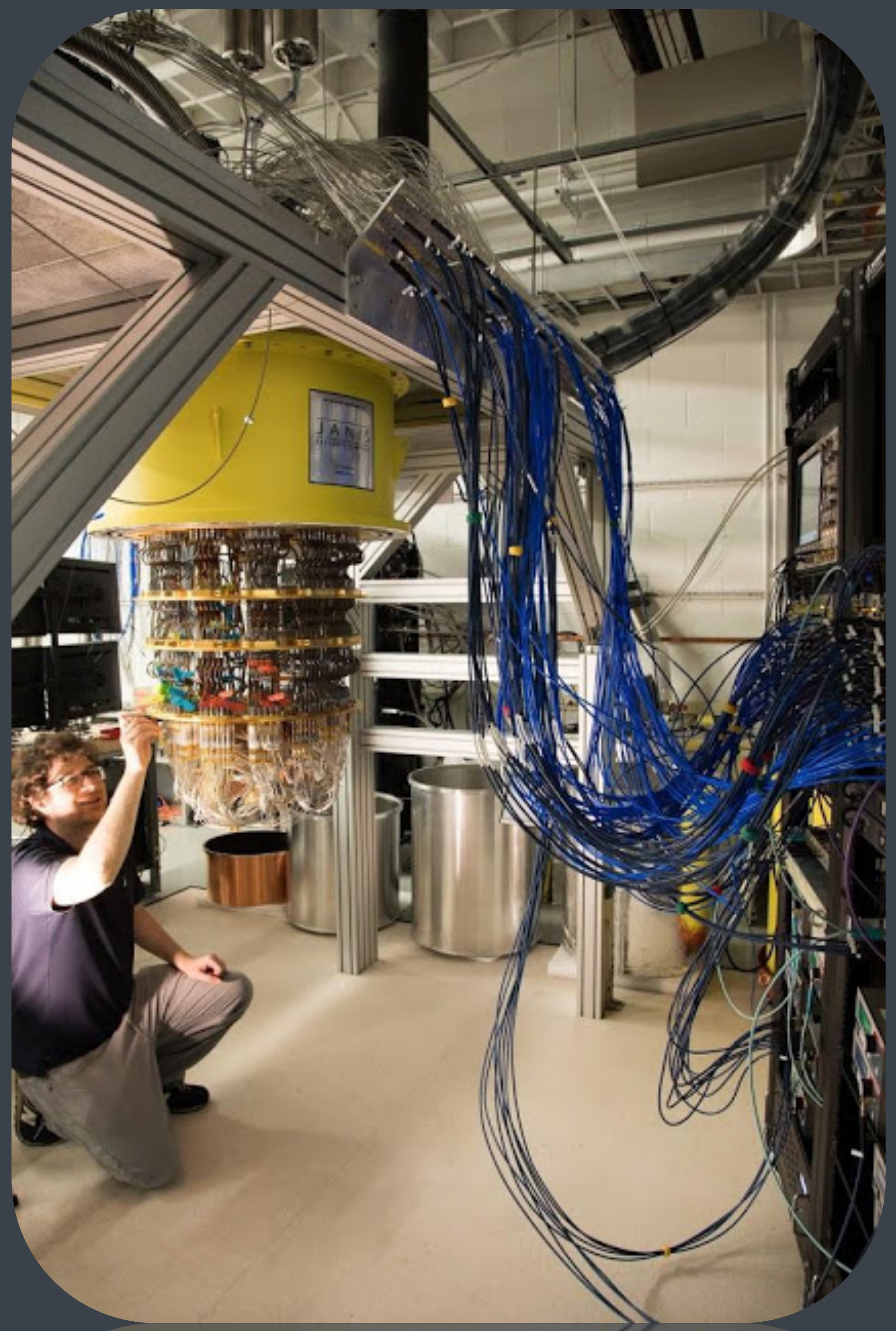


But we learn a lot!

Quantum Computers

But…already now…

IBM has a 5 qubit cloud service
Xanadu has something similar
Rigetti has too
…and probably more



Quantum Computers

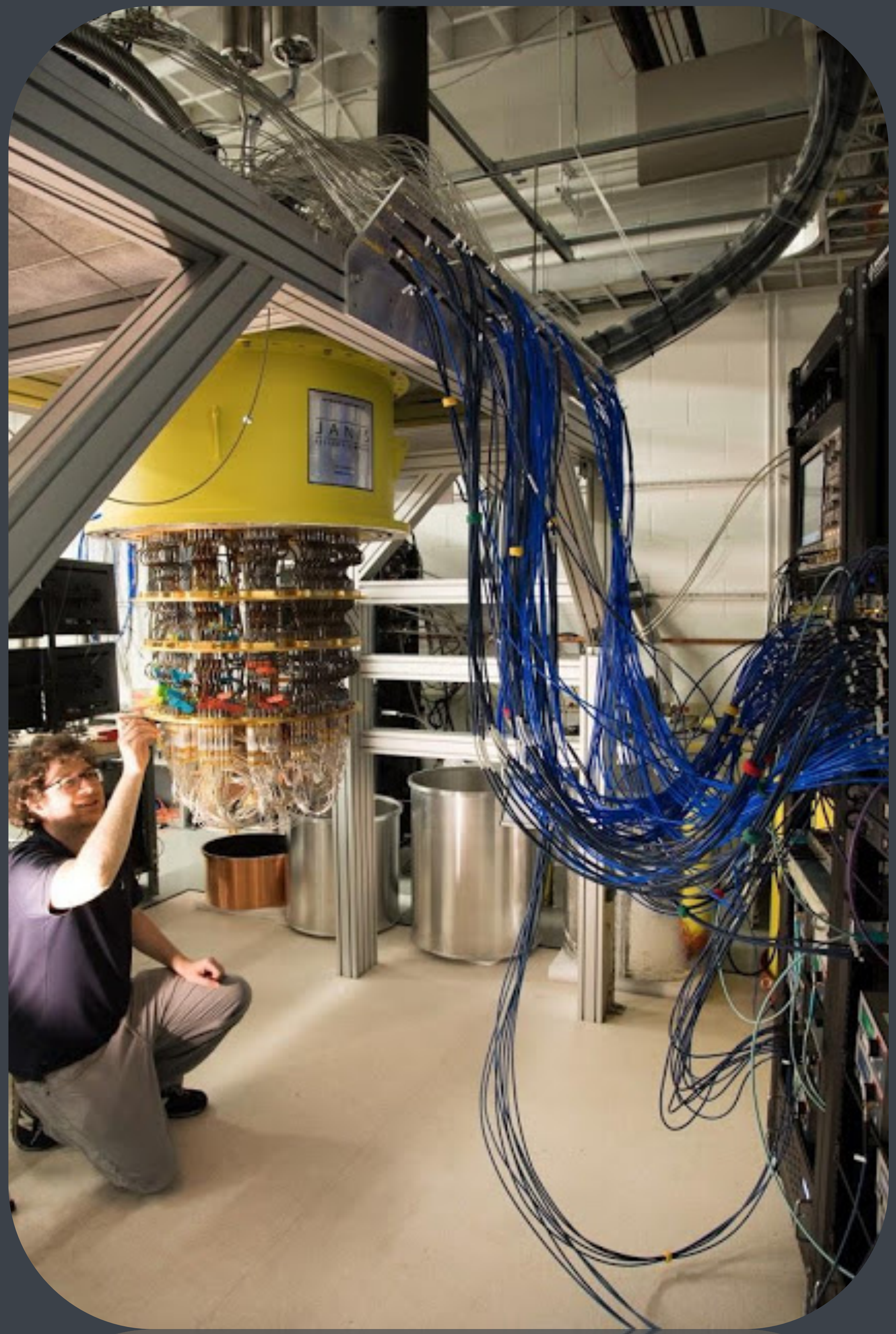
Do they work?

In 2019 Google claimed Quantum Supremacy on a 53 qubit computer: A large, constructed and very academic calculation involving true random numbers was performed in 200 secs.

Google claimed it would take the best super computers 10000 years

IBM proved it could be done in 2.5 days

Nevertheless: **Quantum Supremacy**



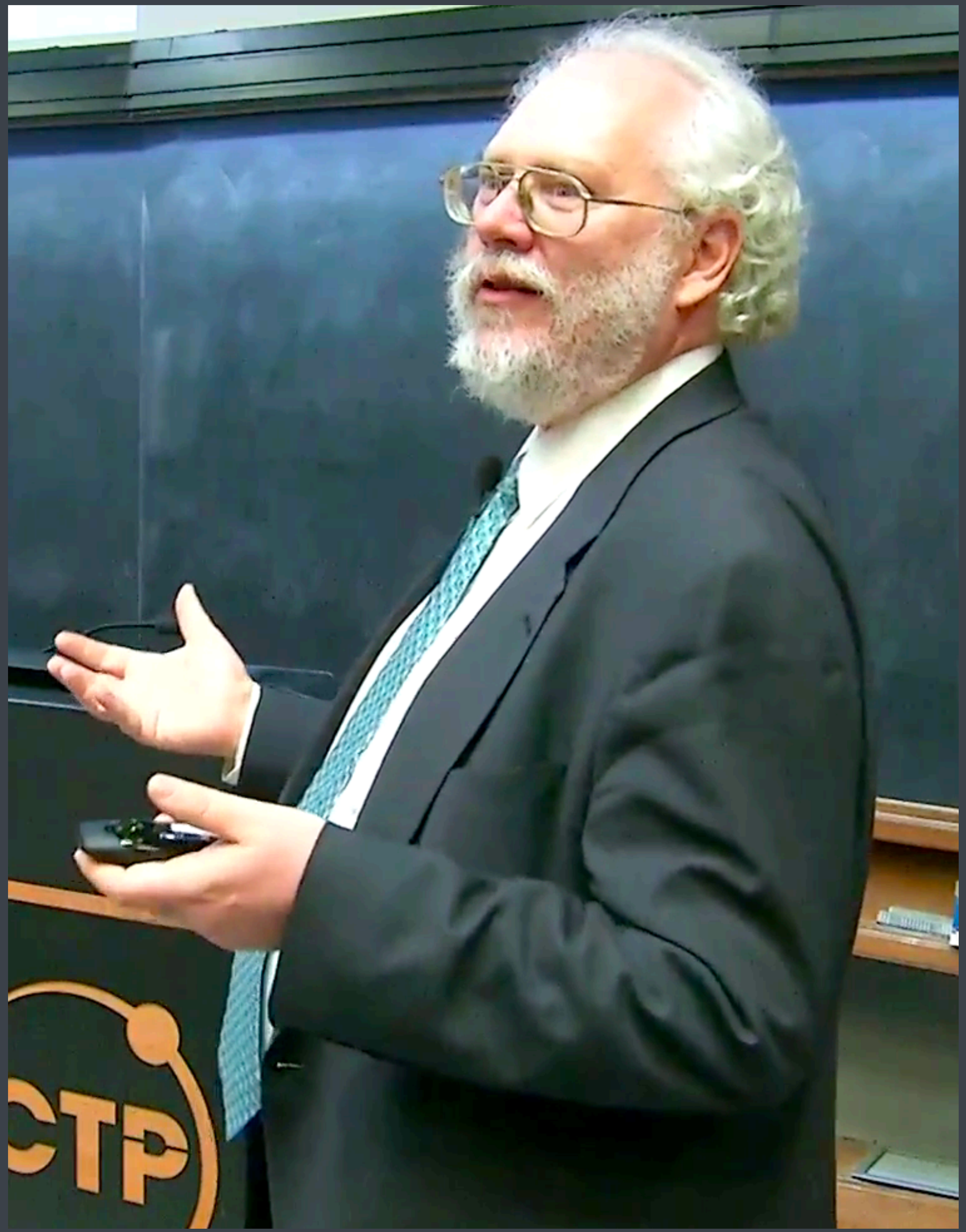
Quantum Computers

In 2001 IBM demonstrated on a 7 qubit computer that 15 with high probability can be broken down into 3 and 5.

Should we care?

Please note!

Shor's algorithm (1994)



(from Wikipedia)

Quantum Computing - Annealing

Finding shortest path, our navigation systems do so every day.

It is finding a global minimum.

Quantum Computing - Annealing

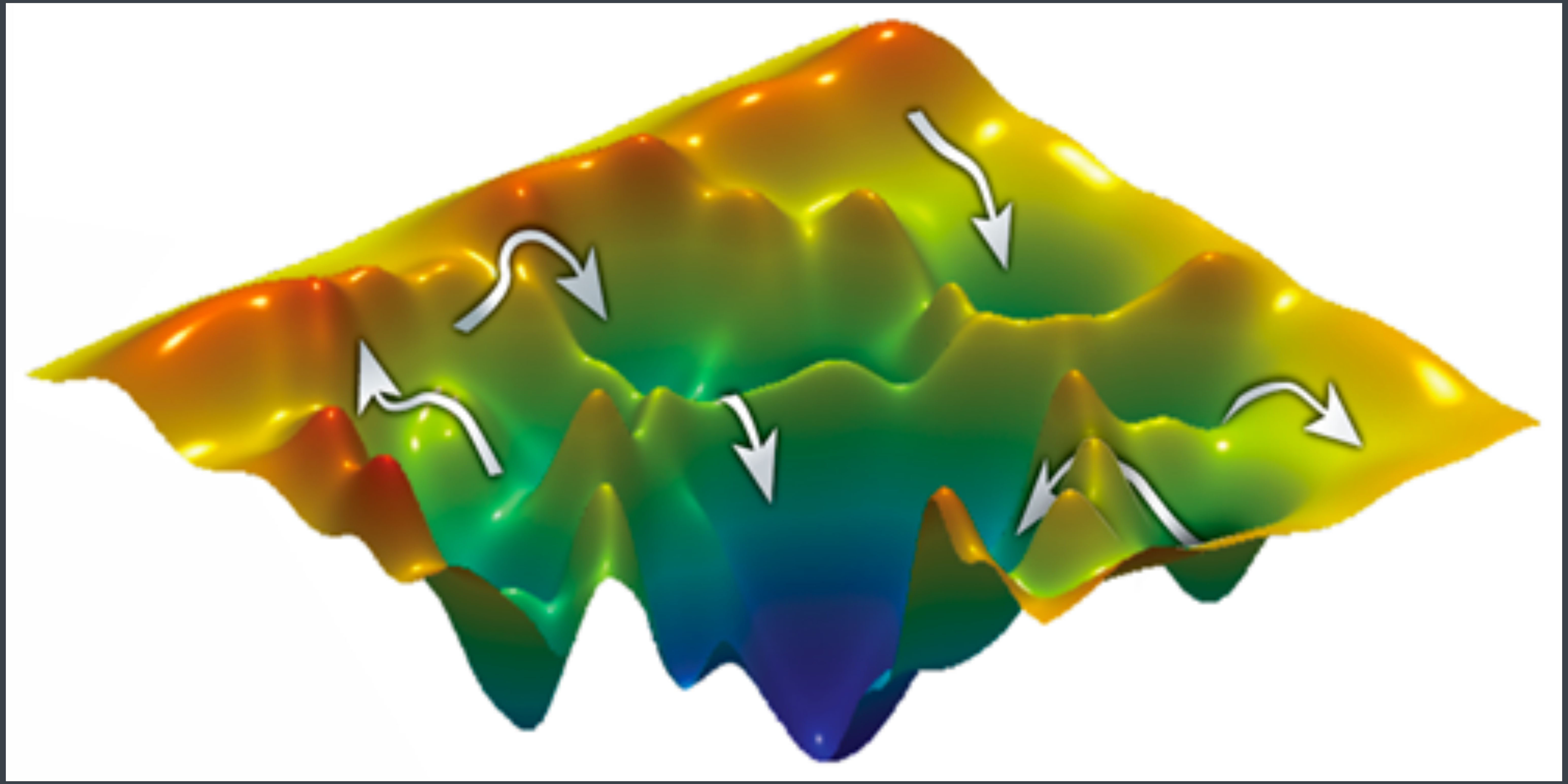
Finding shortest path, our navigation systems do so every day.

It is finding a global minimum.

Imagine if it had more dimensions: It needs to be shortest path matched up against another driver, production constraints, schedules, and more

Like all phenomena in this world, qubits in superposition also like to fall into a mode with lower energy (to seek an energy state with higher entropy)

Quantum Computing - Annealing



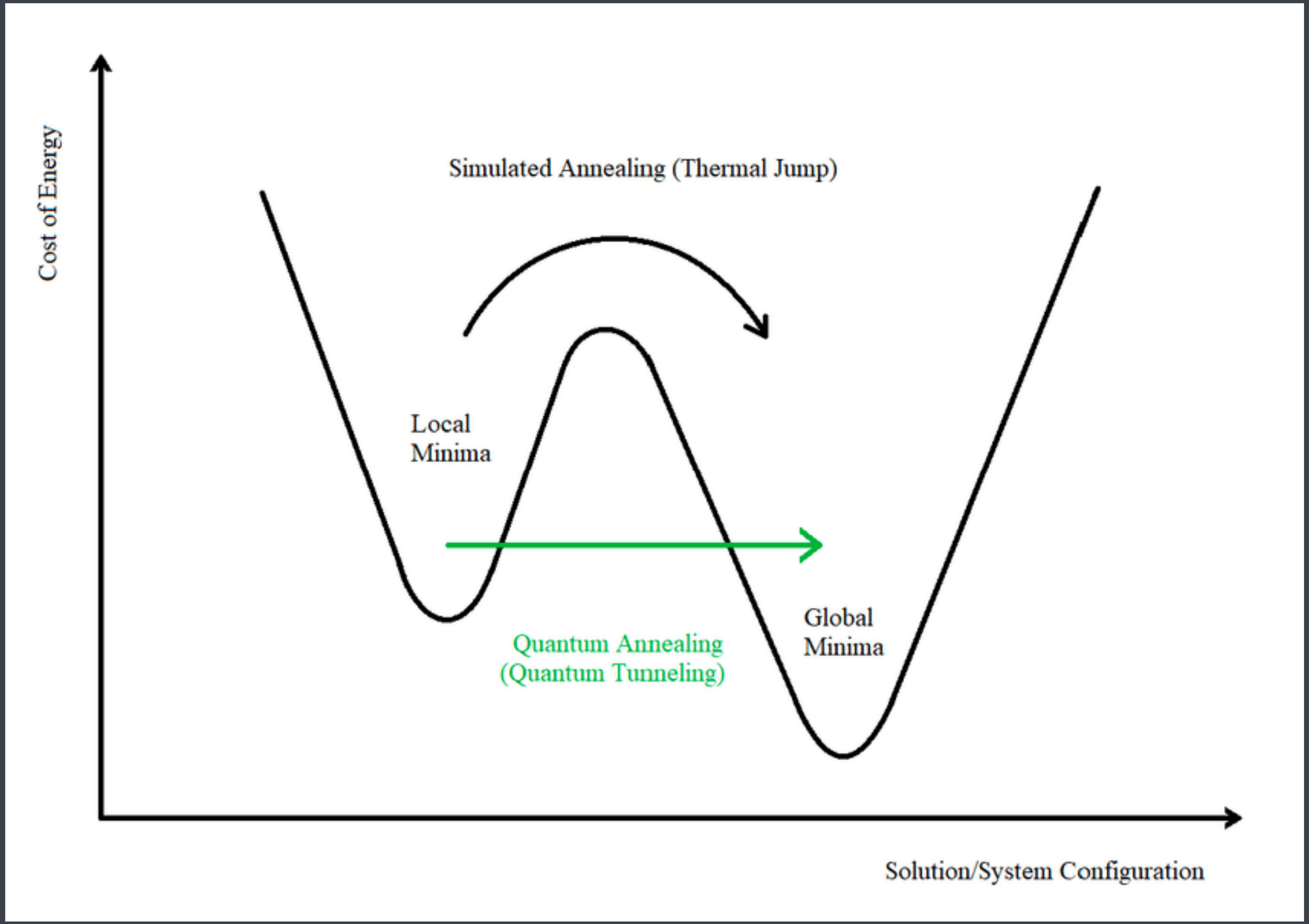
(from physics.aps.org)

TRIFORK.
...think software

Quantum Computing - Annealing

Tunnelling may even help going through walls

The Canadian company
D-Wave Systems
has quantum computers with 5000 qubits specifically designed to do quantum annealing



(from researchgate.org)

Quantum Computing - Annealing

The Canadian company
D-Wave Systems
has quantum computers with 5000 qubits specifically designed to do quantum annealing

(from venturebeat.com)

Wrapping Up

Quantum phenomena is hard to understand because we do not have the language to describe and imagine it.

It can be used for modelling certain types of math problems, but we still haven't been able to build a stable computer to do it.

Quantum annealing is for optimizing problems that relate to finding a global minumum.

Opening Question

Quantum computing: Is it science fiction?

It may be science but it certainly isn’t fiction

Thank You

TRIFORK.
...think software