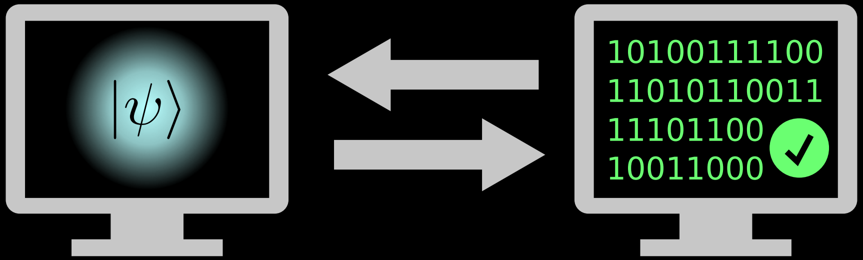


QUANTUM COMPUTING

how to do math with atoms, and how to trust the answers

Greg Kahanamoku-Meyer
PhD candidate, UC Berkeley Physics

Quantum mechanics

Quantum superposition:
“A particle is in multiple places at once.”

Quantum mechanics

Fig. 1: Map of our region

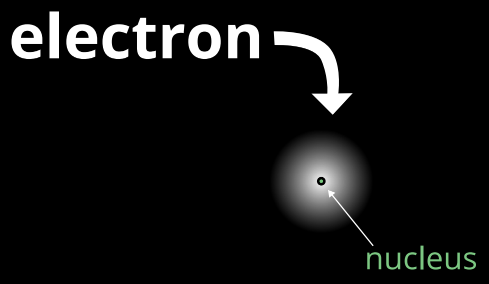


Fig. 2: An atom with 1 electron.

From far away, we can point to the *one* location of Lake Tahoe, and the electron.

Quantum mechanics

Fig. 3: Me and my dog in a lake.

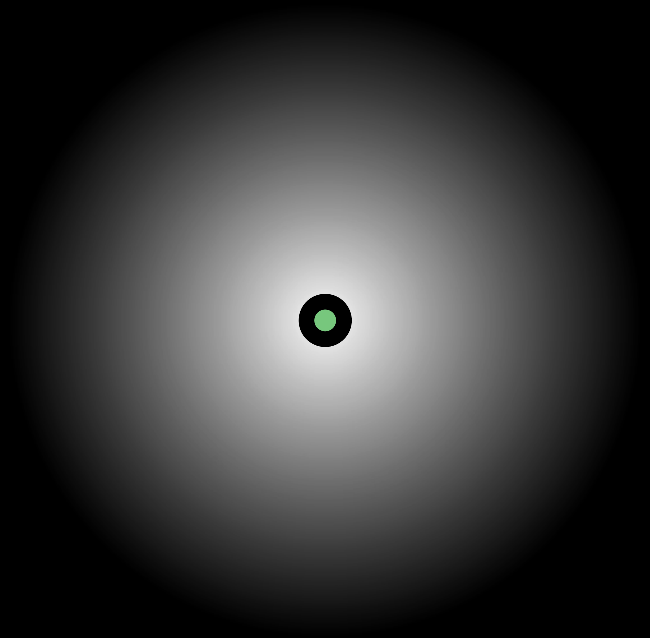


Fig. 4: An atom, close-up.

Up close, “point to the exact position” doesn’t make sense.

Quantum mechanics

Fig. 5: Me and my dog not in a lake.

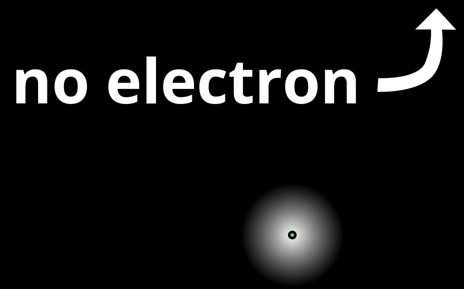


Fig. 6: Not where the electron is.

… but there are definitely wrong answers.

Wavefunctions

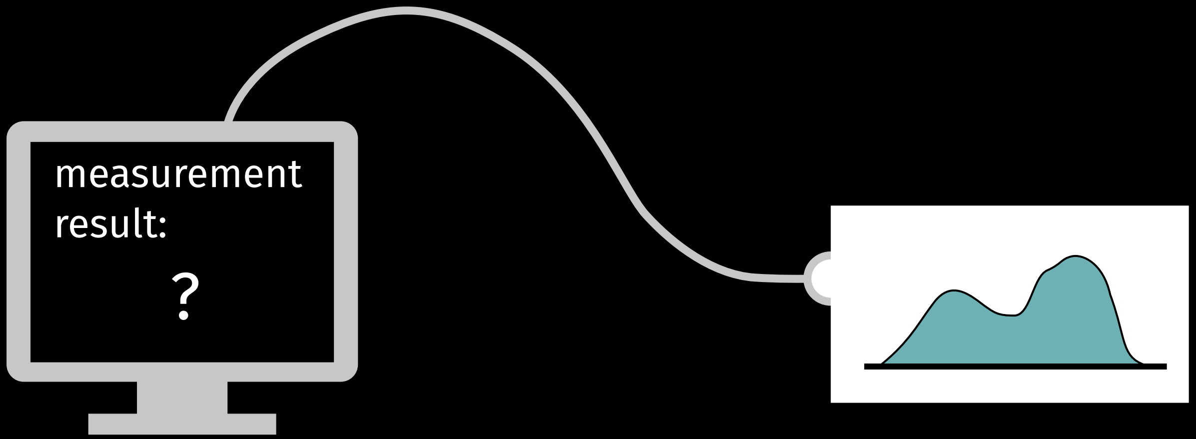
Before measuring position　　　　After measuring position

Fig. 7: Wavefunctions of a particle.

“Wave-particle duality” → “Wave-‘more pointy wave’ duality”

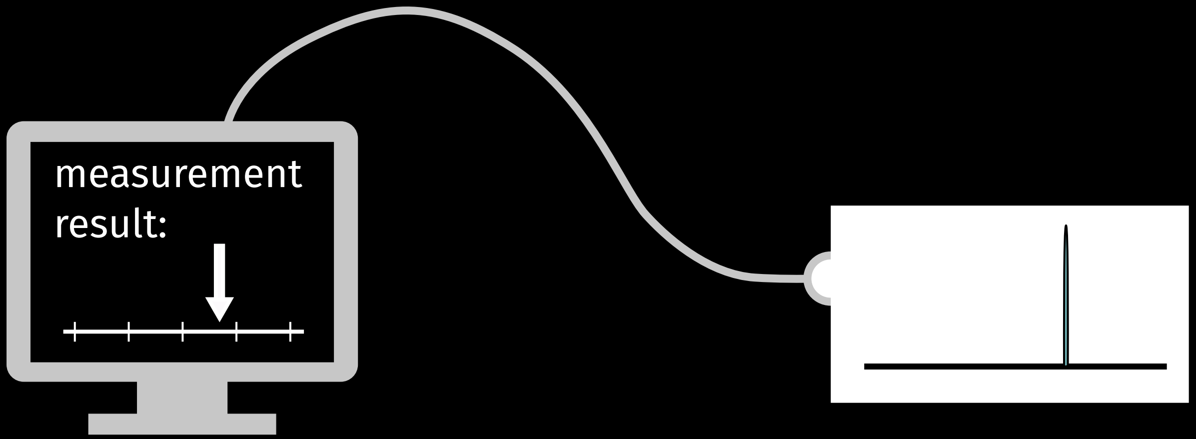
What is a “measurement”?

Roughly: anytime something “big” depends on what the quantum object is doing.



What is a "measurement"?

Roughly: anytime something "big" depends on what the quantum object is doing.

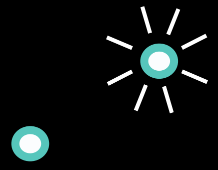


More than just “where a particle is”

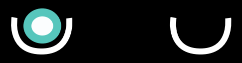
Anything you can measure about a particle behaves this way!

For simplicity, look at measurements with only two options:

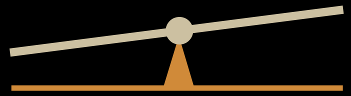
Direction of rotation



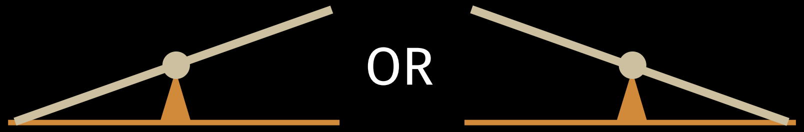
Energy level



Position (when confined)



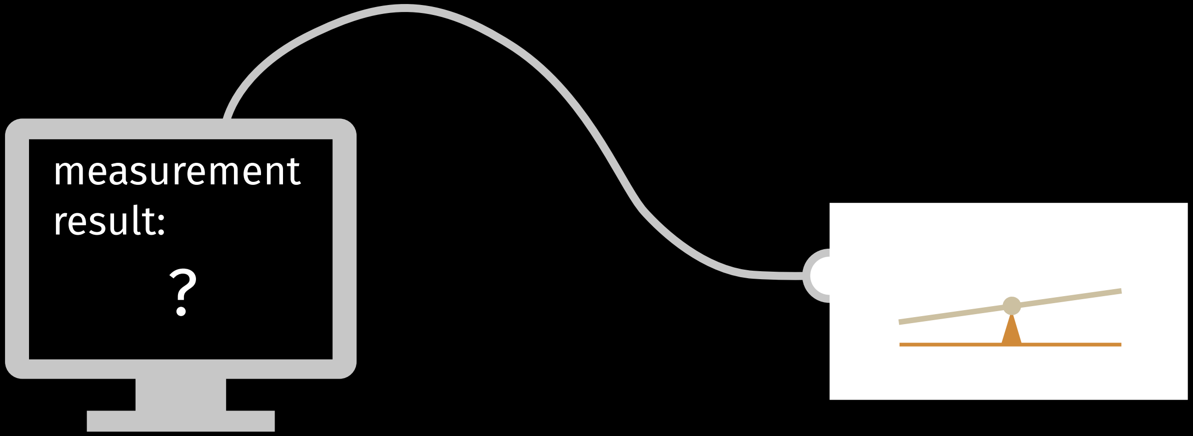
Before measurement



After measurement

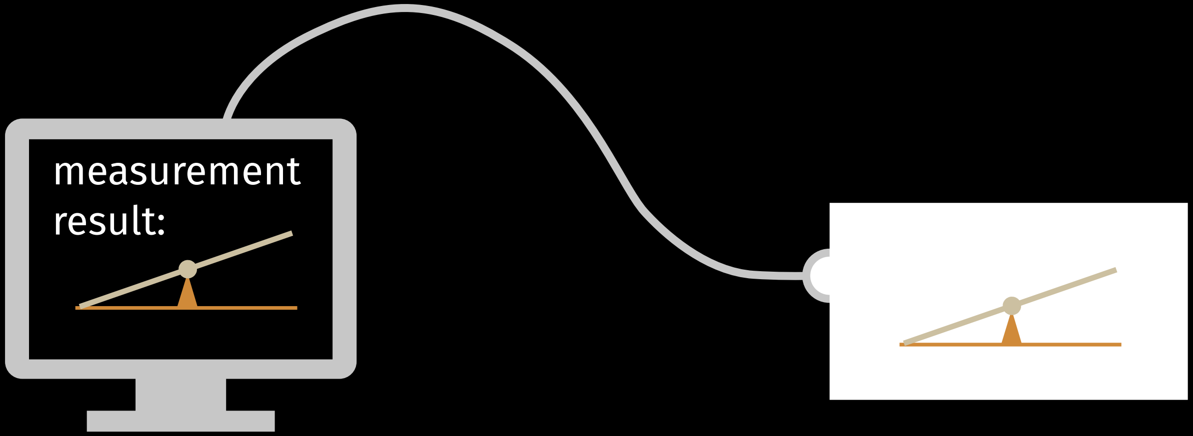
What is a “measurement”?

Roughly: anytime something “big” depends on what the quantum object is doing.

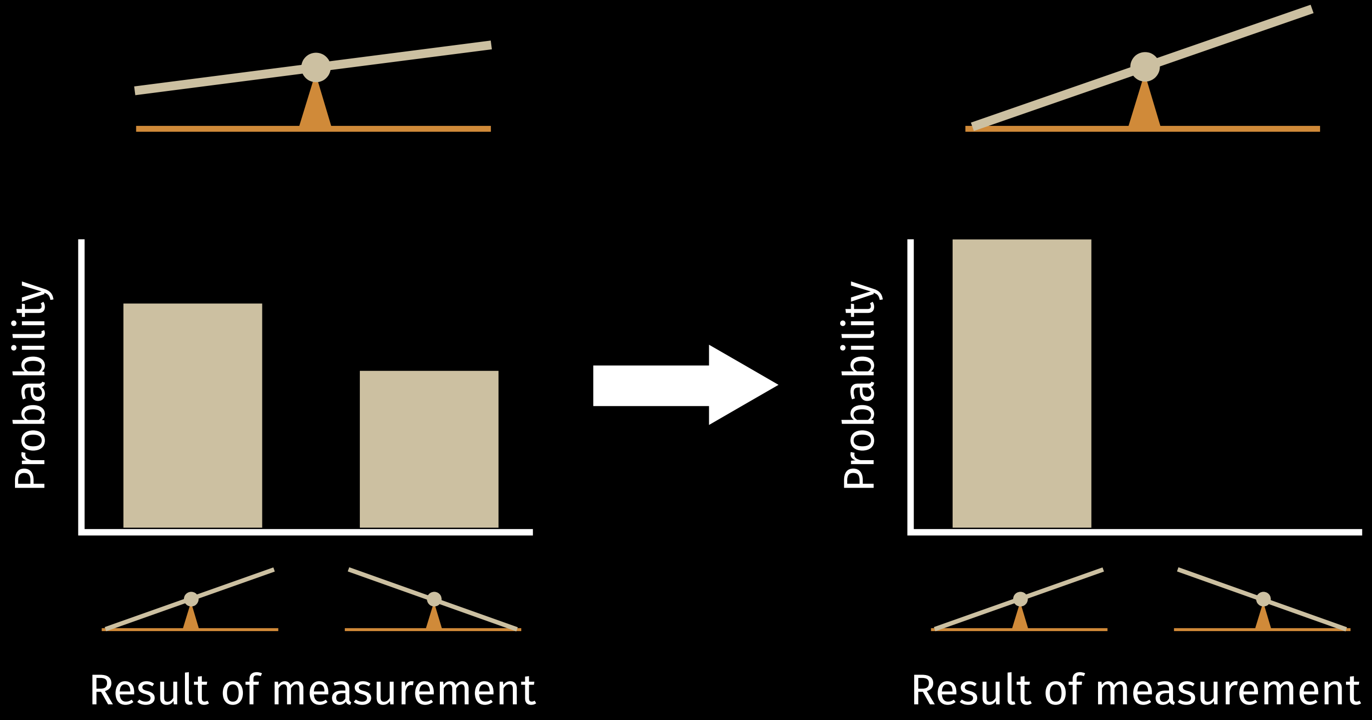


What is a “measurement”?

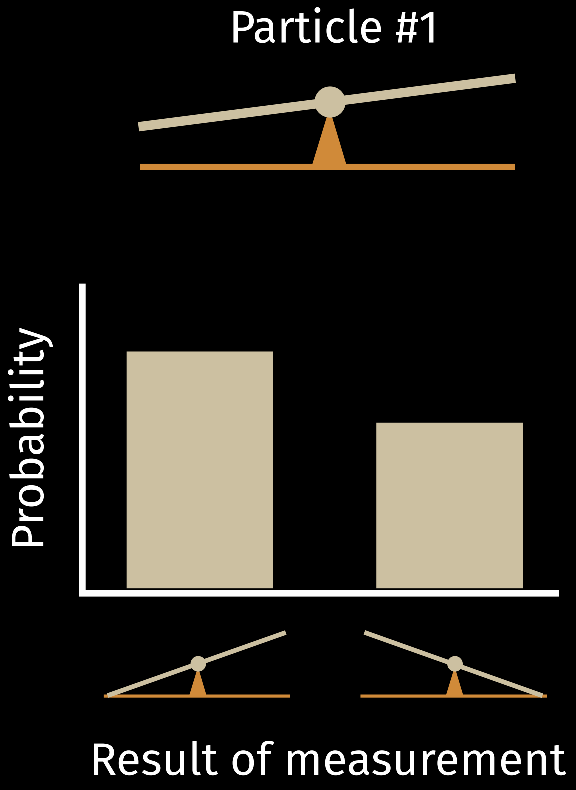
Roughly: anytime something “big” depends on what the quantum object is doing.

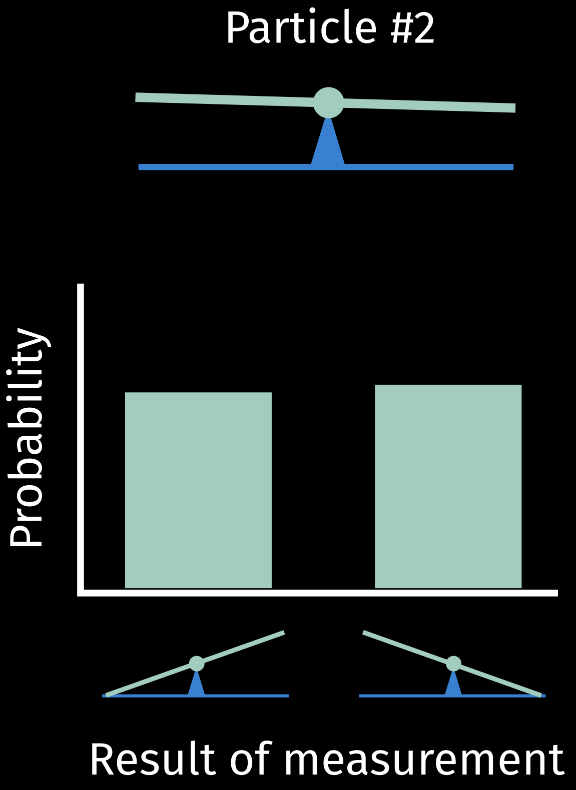


What determines the result?

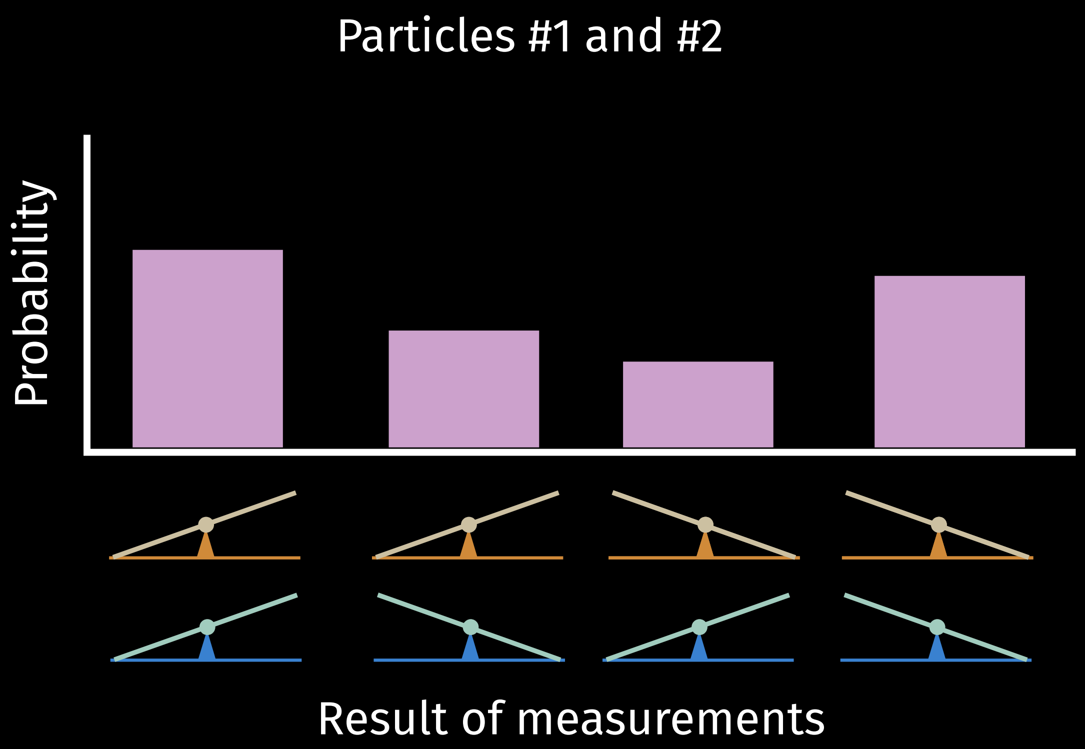


More than one quantum object

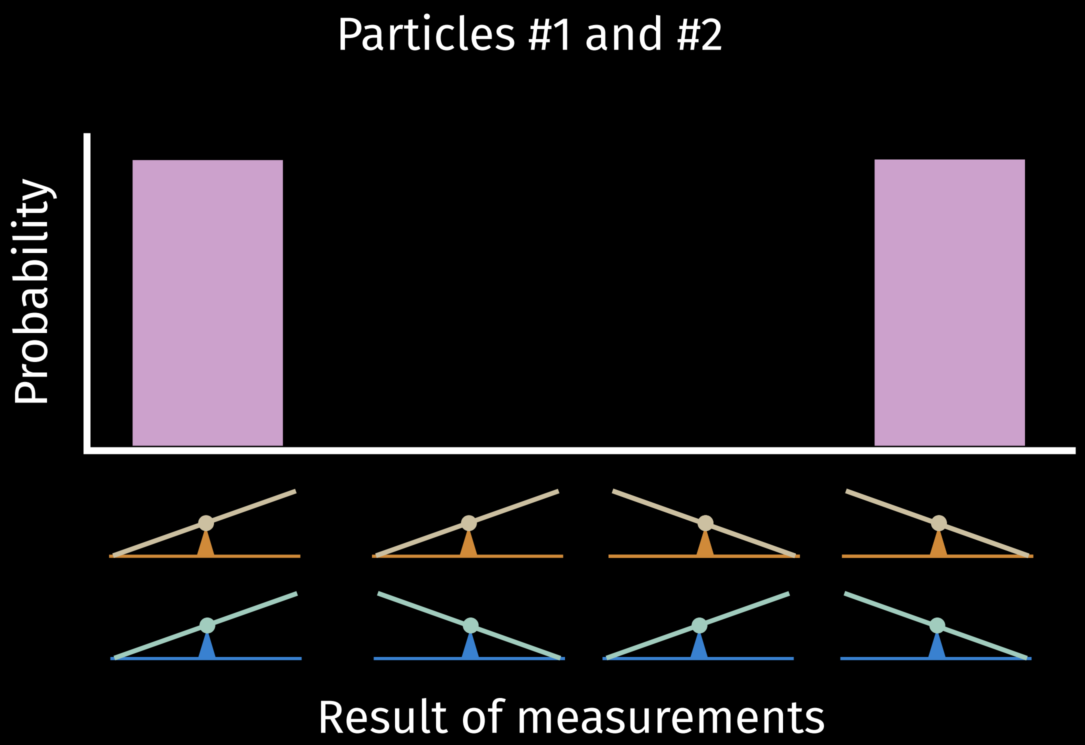




More than one quantum object



More than one quantum object

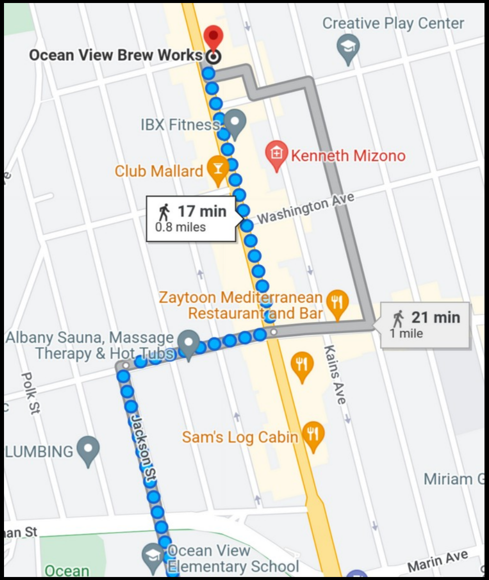


This is **quantum entanglement**---the outcomes are *connected*.

Computers

What is a computer?

Instagram: ads with occasional pictures of your friends



Google Maps: ads along with directions to beer

Computers

What is a computer?

At a low level, a computer is just a **fancy calculator**

Computers

What is a computer?

Uses physical systems (electricity in tiny wires, tiny magnets on a disk, etc.) to store data and do math on it

Computers

What is a computer?

Those physical things represent **bits**: values that can be 0 or 1

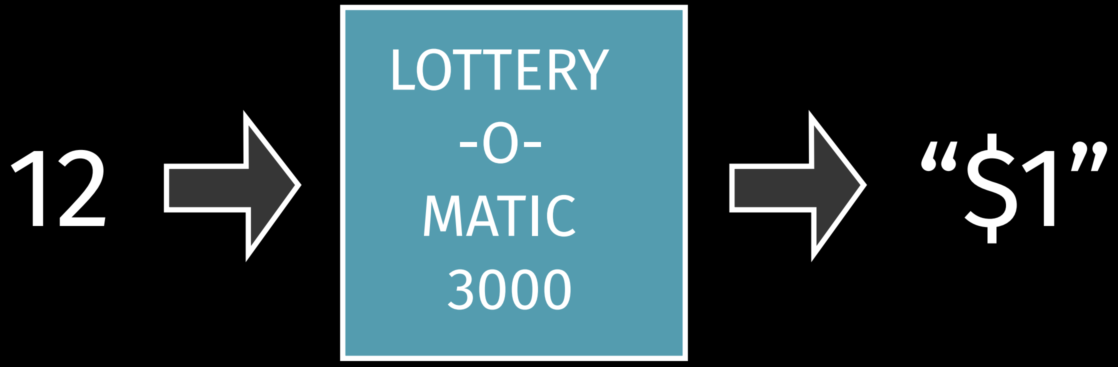
Computers

What is a computer?

What if we replaced those tiny physical pieces with something quantum?
Quantum bits → "qubits"

Quantum computing: hacking the lottery

We have our hands on the code behind the lottery:
takes in a number, and computes the payout!



Quantum computing: hacking the lottery

We have our hands on the code behind the lottery:
takes in a number, and computes the payout!

5041 → LOTTERY -O- MATIC 3000 → "$0"

Quantum computing: hacking the lottery

We have our hands on the code behind the lottery:
takes in a number, and computes the payout!

??????? → LOTTERY -O- MATIC 3000 → "$1,000,000"

<u>Goal: find the one number that gives "$1,000,000"</u>

Regular ("classical") computer

Best strategy: … just try every number

Quantum computing: hacking the lottery

Goal: find the one number that gives “$1,000,000”

{ 0
1
2
3
…
512484

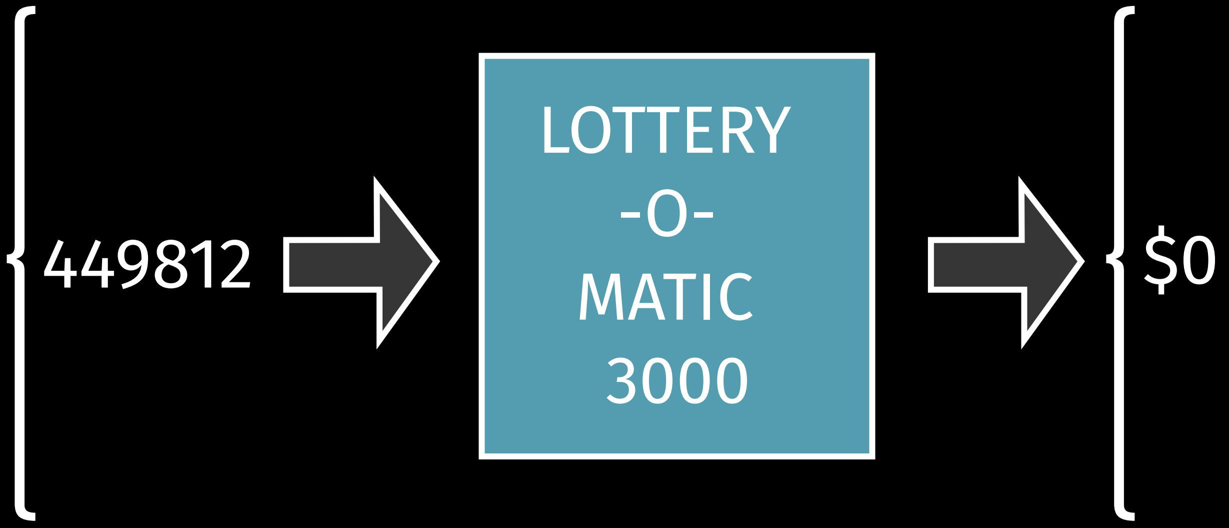
LOTTERY
-O-
MATIC
3000

{ $0
$0
$1
$0
…
$1,000,000

{ means quantum superposition

Quantum computing: hacking the lottery

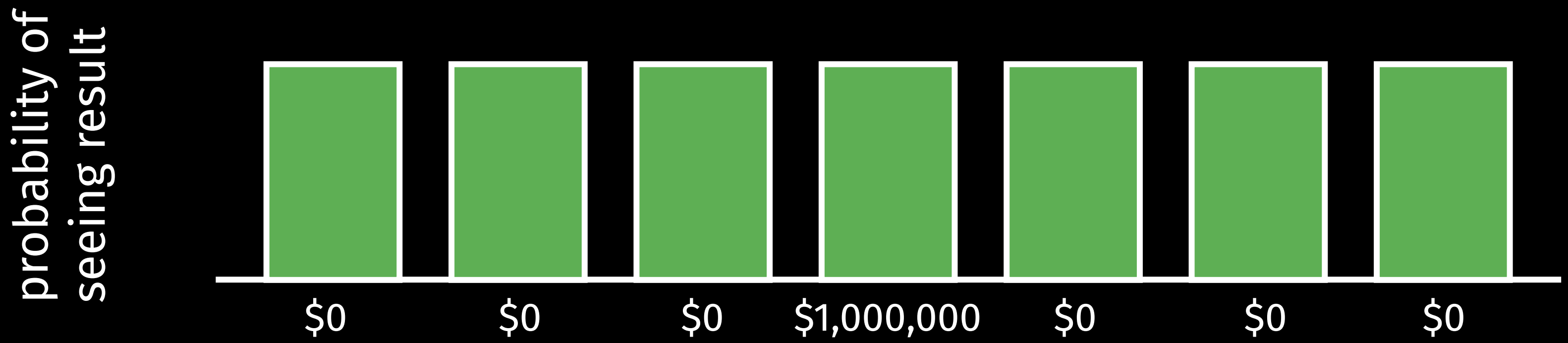
We did the calculation, now let’s look at the results!! And we get…



Quantum input → quantum output!

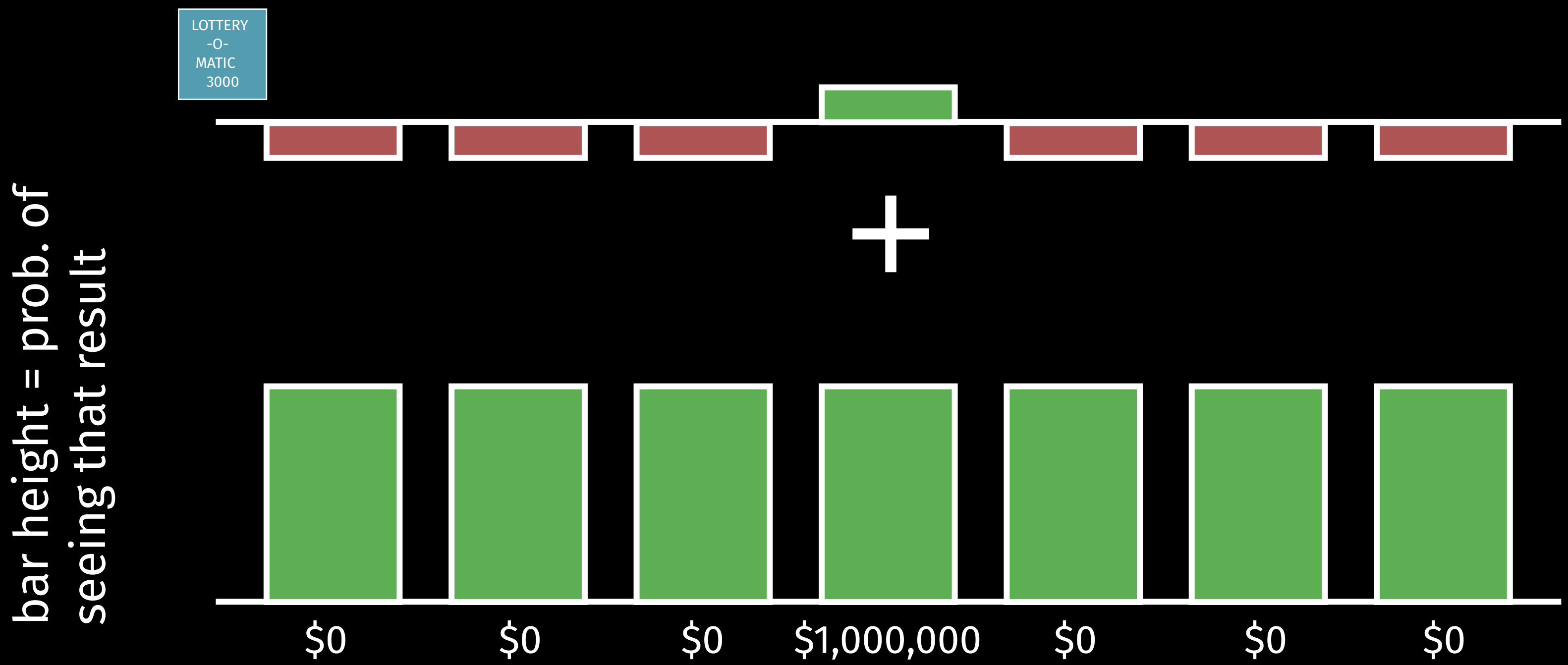
Quantum computing: hacking the lottery

Goal: find the one number that gives “$1,000,000”



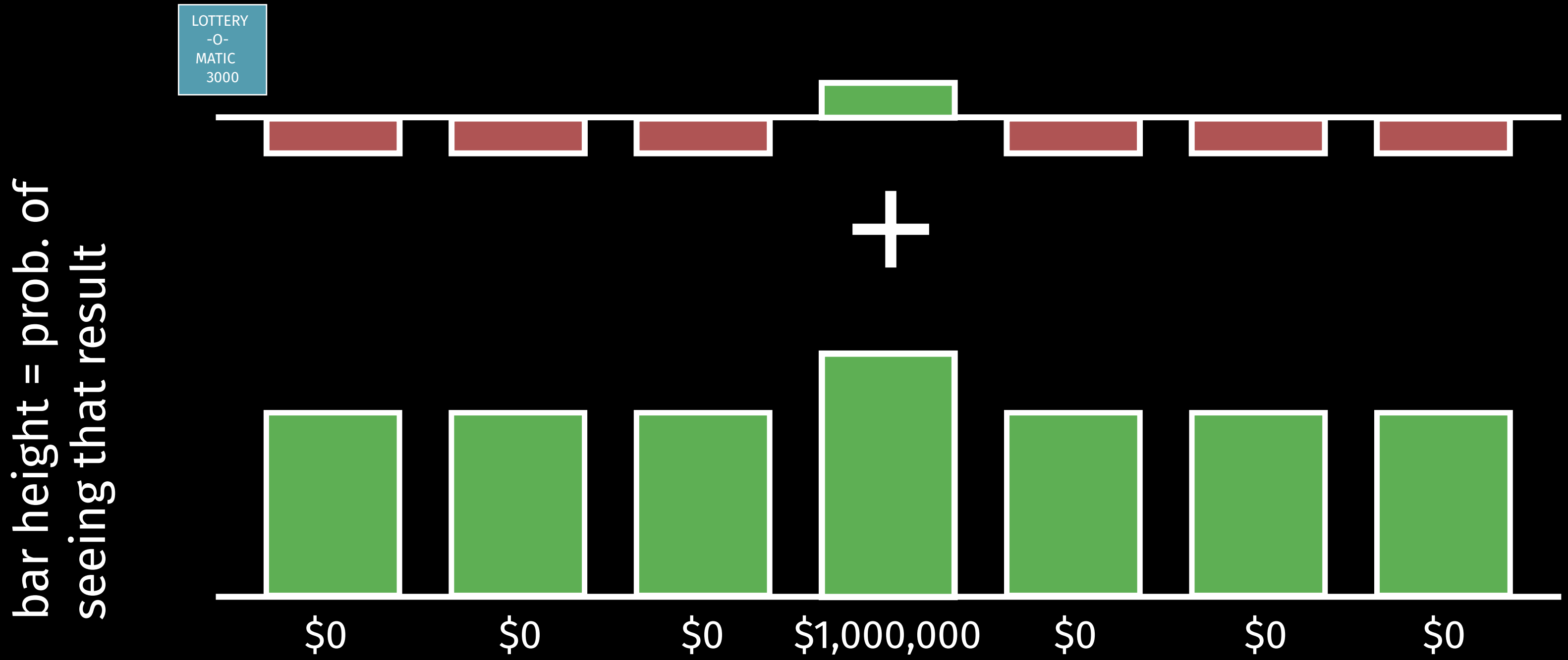
Quantum computing: hacking the lottery

Goal: find the one number that gives "$1,000,000"



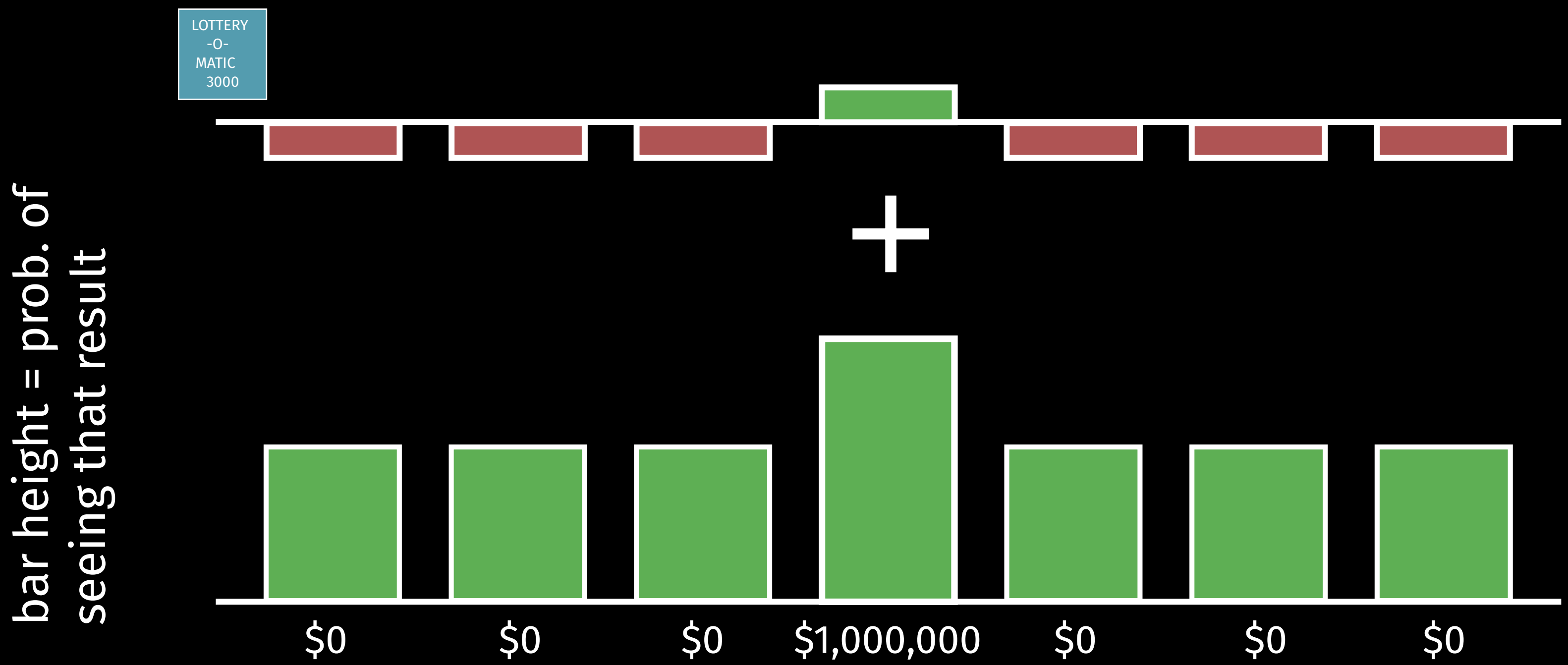
Quantum computing: hacking the lottery

Goal: find the one number that gives "$1,000,000"



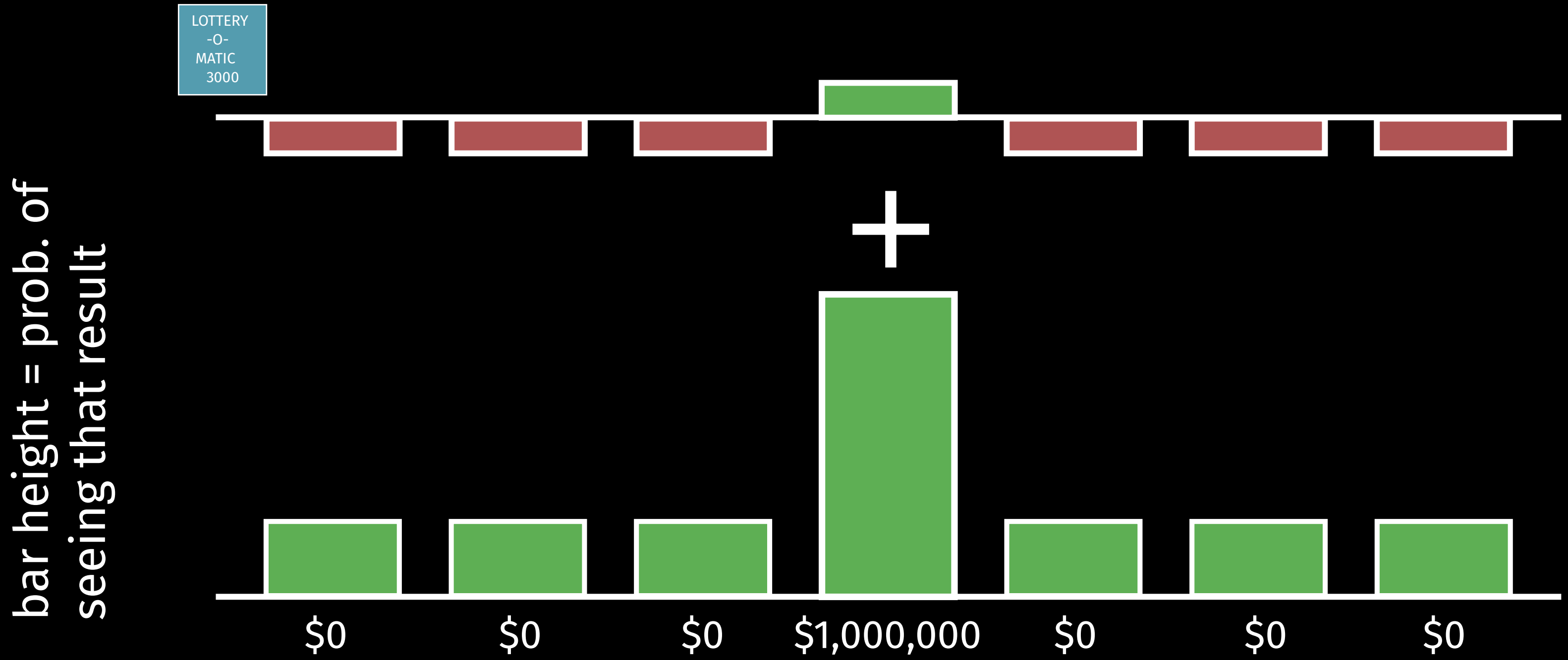
Quantum computing: hacking the lottery

Goal: find the one number that gives "$1,000,000"



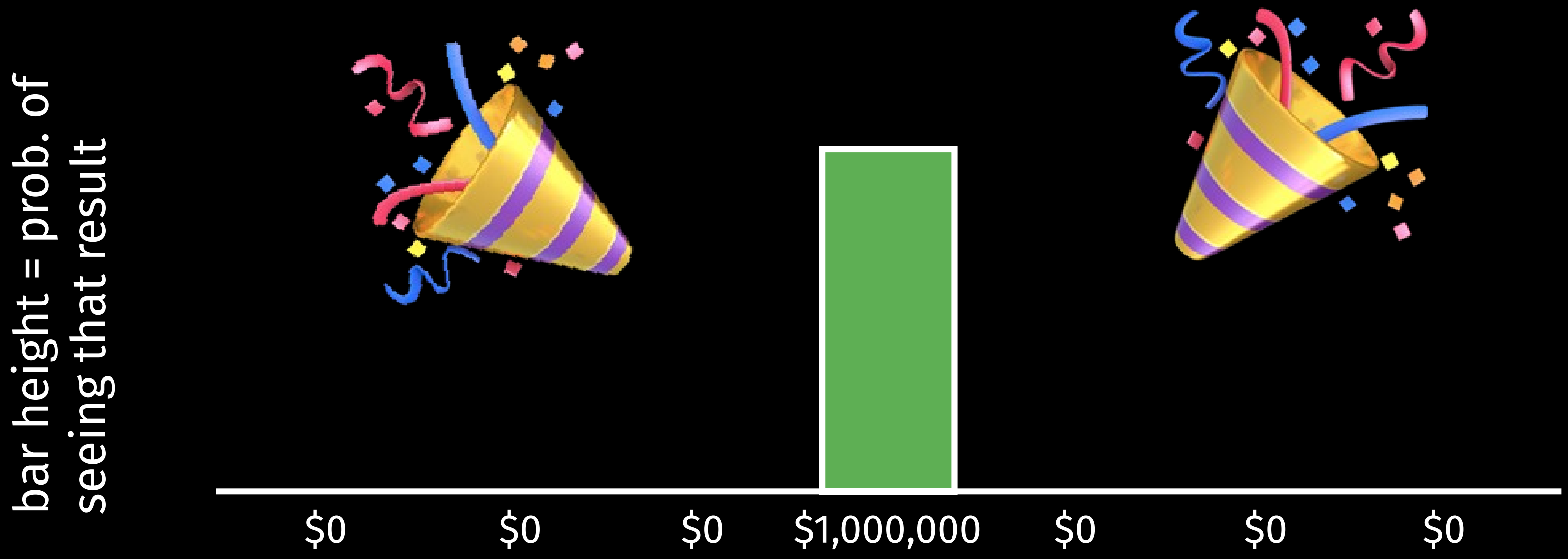
Quantum computing: hacking the lottery

Goal: find the one number that gives “$1,000,000”



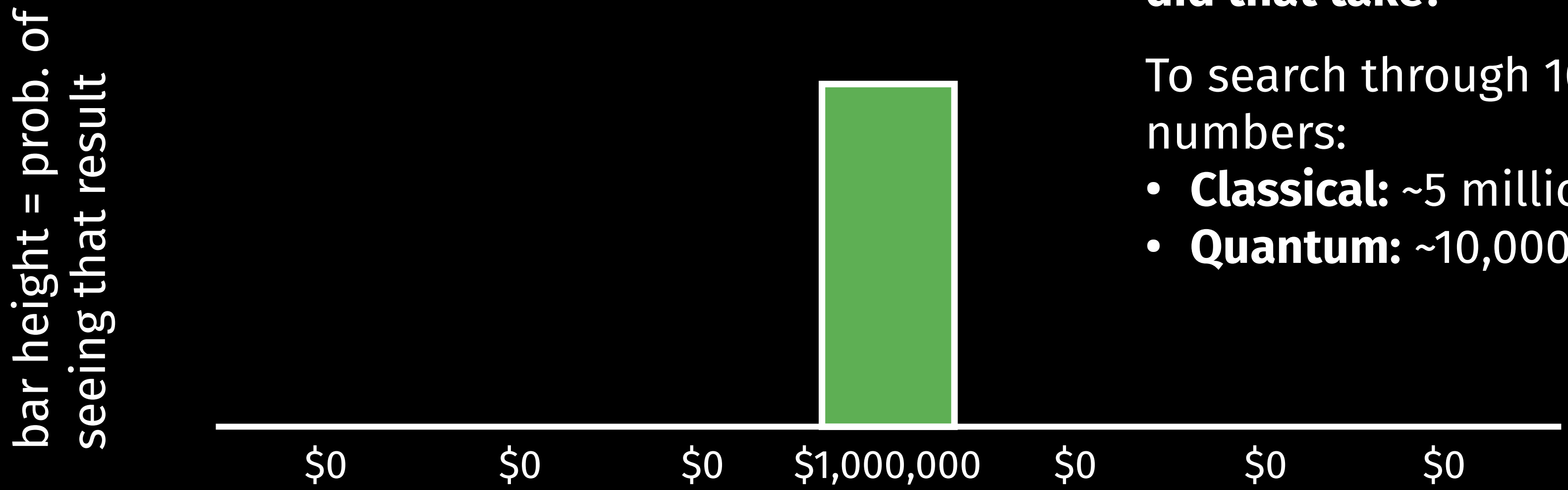
Quantum computing: hacking the lottery

Goal: find the one number that gives “$1,000,000”



Quantum computing: hacking the lottery

Goal: find the one number that gives "$1,000,000"



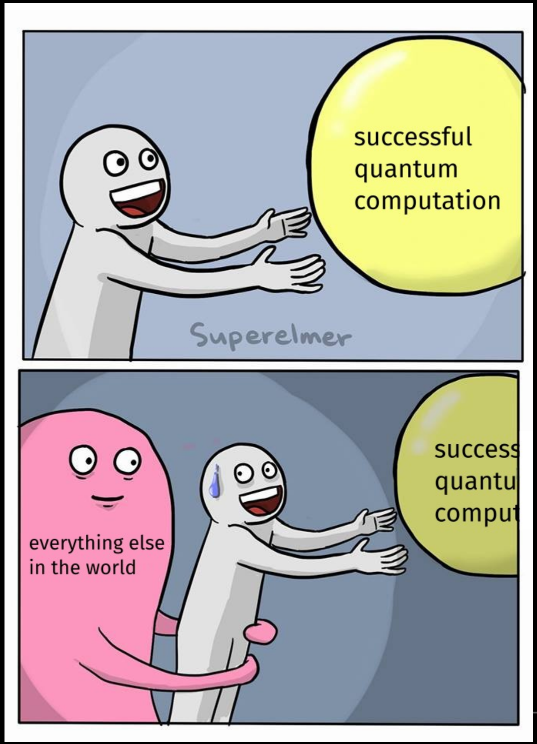
How many uses of LOTTERY -O- MATIC 3000 **did that take?**

To search through 10 million numbers:

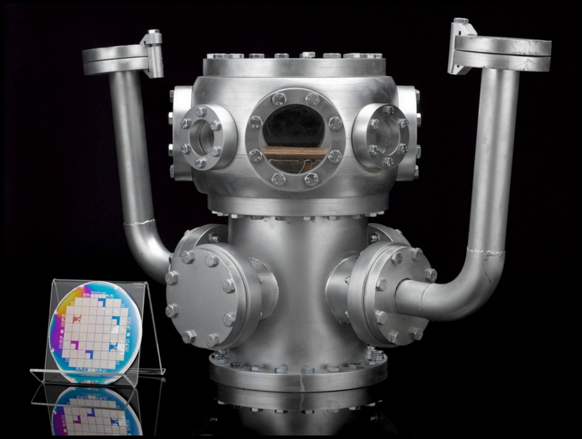
- **Classical:** ~5 million
- **Quantum:** ~10,000

Why aren't we doing this right now

Major difficulty #1: quantum computations are *fragile*



If *anything* interacts into the qubits, the computation breaks!



Why aren’t we doing this right now

Major difficulty #2: quantum computers are *slow*

“Grover search” (hacking the lottery)

Quantum

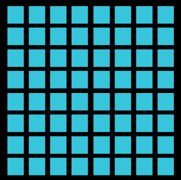
Classical

Why aren’t we doing this right now

Major difficulty #2: quantum computers are *slow*

“Grover search” (hacking the lottery)

Quantum



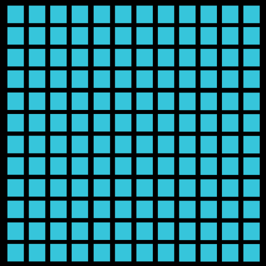
Classical

Why aren’t we doing this right now

Major difficulty #2: quantum computers are *slow*

“Grover search” (hacking the lottery)

Quantum



Classical

Why aren’t we doing this right now

Major difficulty #2: quantum computers are *slow*

“Grover search” (hacking the lottery)

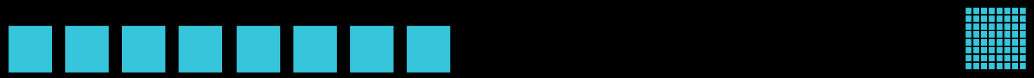
Quantum

Classical

Why aren’t we doing this right now

Major difficulty #2: quantum computers are *slow*

“Grover search” (hacking the lottery)



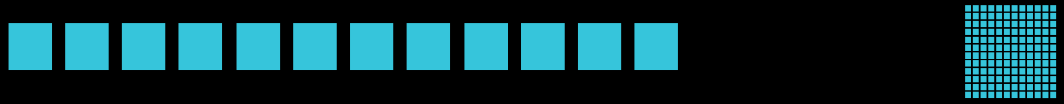
Quantum

Classical

Why aren't we doing this right now

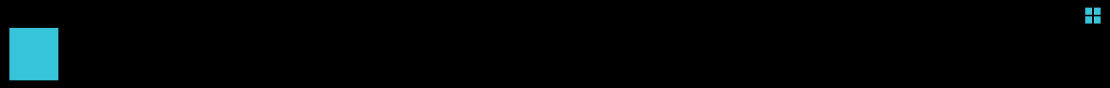
Major difficulty #2: quantum computers are *slow*

"Grover search" (hacking the lottery)



Quantum Classical

Some hope: exponential speedups



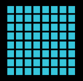
Quantum Classical

Some hope: exponential speedups

Quantum

Classical

Some hope: exponential speedups

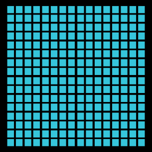


Quantum

Classical

Some hope: exponential speedups

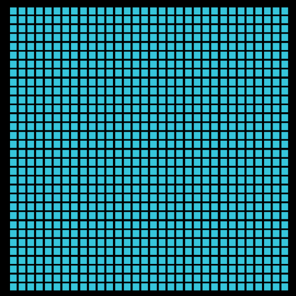
Quantum



Classical

Some hope: exponential speedups

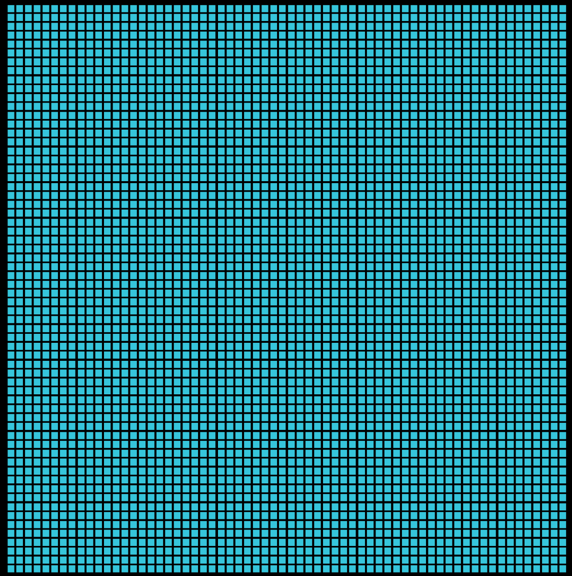
Quantum



Classical

Some hope: exponential* speedups

Quantum



Classical

Challenge: bigger quantum computations → more fragile

What quantum computers can do

Current state of the art:
For an extremely specific set of calculations,
the best quantum computers can *probably* beat a
classical supercomputer.

For most **useful** tasks, they don't
beat the computer chip in my toaster.

Summary of quantum speedups

Task	**Theoretical speedup**	**Can we do it in 2022?**
Searching (lottery)	Somewhat faster	Too small and fragile

Summary of quantum speedups

Task	Theoretical speedup	Can we do it in 2022?
Searching (lottery)	Somewhat faster	Too small and fragile
Factoring numbers	Much faster	Too small and fragile

Summary of quantum speedups

Task	Theoretical speedup	Can we do it in 2022?
Searching (lottery)	Somewhat faster	Too small and fragile
Factoring numbers	Much faster	Too small and fragile
Machine learning	Not clear (and depends on what you're doing)	Too small and fragile

Summary of quantum speedups

Task	Theoretical speedup	Can we do it in 2022?
Searching (lottery)	Somewhat faster	Too small and fragile
Factoring numbers	Much faster	Too small and fragile
Machine learning	Not clear (and depends on what you’re doing)	Too small and fragile
Chemistry calculations	Not clear (and depends on what you’re doing)	Too small and fragile

Summary of quantum speedups

Task	Theoretical speedup	Can we do it in 2022?
Searching (lottery)	Somewhat faster	Too small and fragile
Factoring numbers	Much faster	Too small and fragile
Machine learning	Not clear (and depends on what you’re doing)	Too small and fragile
Chemistry calculations	Not clear (and depends on what you’re doing)	Too small and fragile
Certain quantum mechanics problems	Exponentially faster, depending on the problem	Experiments seem to have beaten regular computers

Side note: factoring

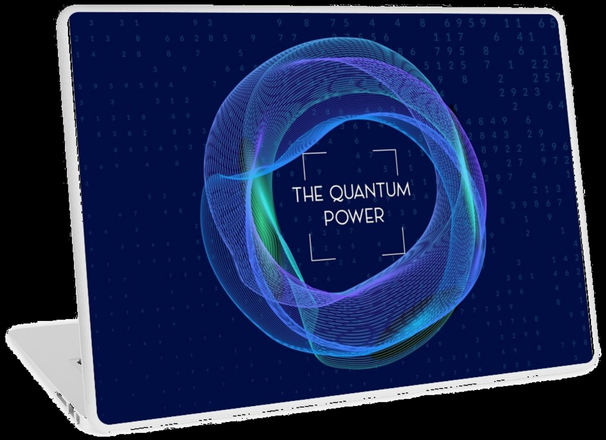
The security of basically the *entire internet* relies on factoring (and related problems) being hard.

What you get if you search the web for "quantum hacker"

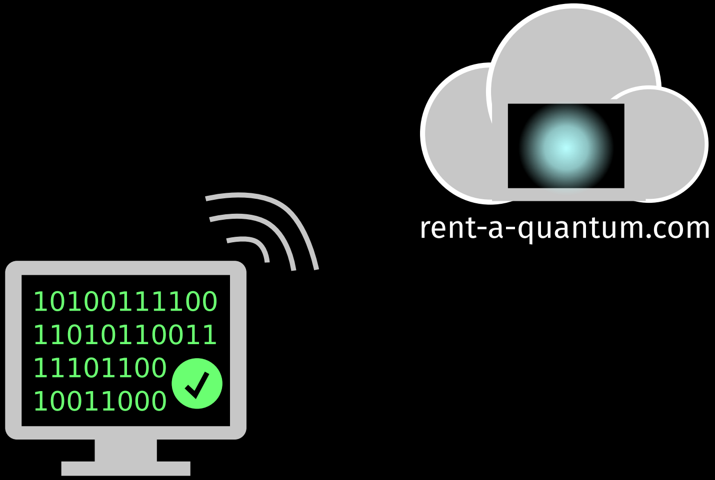
Features of current quantum computers

- Slow
- Small
- Extremely error prone
- Algorithms are thought to be better than regular computers… for a few very specific problems
- **We don’t know the limits of their capabilities yet!**

The future of quantum computing



A quantum laptop? Probably not.



Quantum cloud service? Probably!

Trusting quantum computers

Q: Why can't you trust atoms?

A: Because they make up everything!

Trusting quantum computers

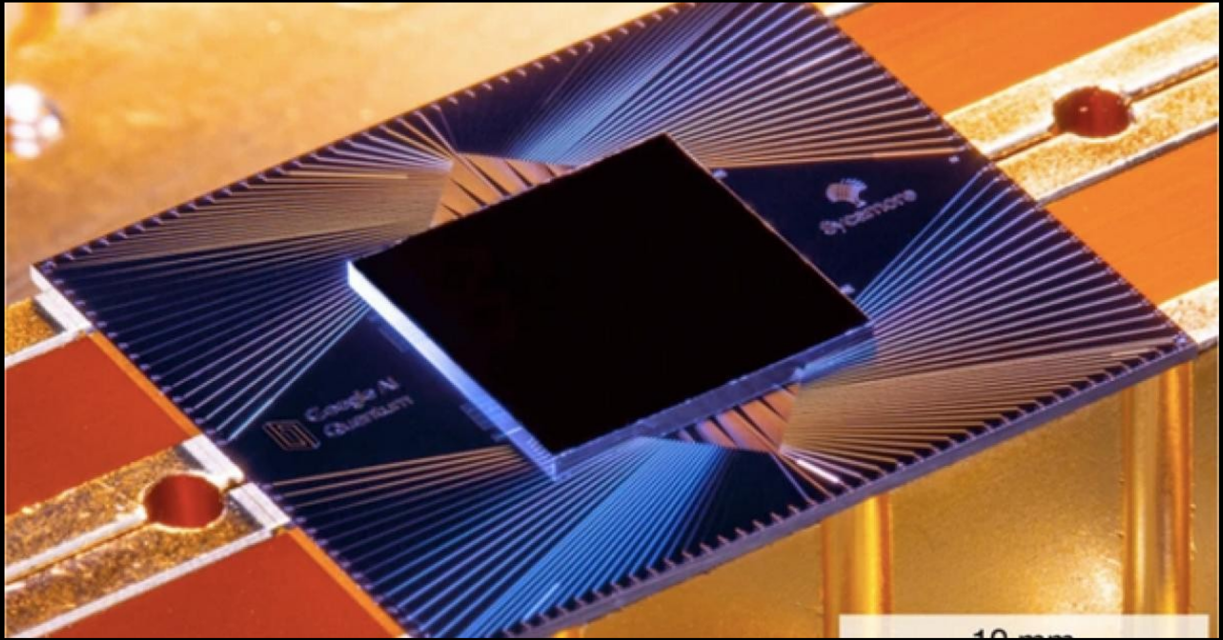
Q: Why can't you trust atoms?

~~A: Because they make up everything!~~

If regular computers can't solve the problem,
how do we check that the answer is *right*?

Trusting quantum computers

Just checking if it's working: check all of the special cases you can find



The 53-qubit processor Google used to show the first "quantum advantage"

Trusting quantum computers

Just checking if it's working: check all of the special cases you can find

nature

Explore content ⌄ About the journal ⌄ Publish with us ⌄

nature > articles > article

Article | Published: 23 October 2019

Quantum supremacy using a programmable superconducting processor

Frank Arute, Kunal Arya, … John M. Martinis + Show authors

Nature **574**, 505–510 (2019) | Cite this article

923k Accesses | **2207** Citations | **6222** Altmetric | Metrics

Trusting quantum computers

Thursday, August 4, 2022
Today's Paper

The New York Times

World U.S. Politics N.Y. Business Opinion Tech Science Health Sports Arts Books

Theranos Leaves Biotech Business, Turns to Building Quantum Computers

- CEO Elizabeth Holmes states the emerging field of quantum computing will be a "new start" for the company
- Despite extensive fraud at previous company, investors inexplicably believe it's a good idea to dump millions of dollars into this new venture

To be clear, this is not a real headline. I made it up.

How do we verify the results of a quantum computer *we don't trust*?

Some problems are easy to check!

Factoring

15

=

3 x 5

Multiplication

Some problems are easy to check!

Factoring

HARD

58592674796345200961477663

=

8839985805991 x 6628141275593

Multiplication

EASY

What about the problems that aren't?

Demo: proving that you can distinguish colors

Summary

- Quantum computers are faster, but in subtle ways and only for specific problems
- Current quantum computers are small, slow, and error-prone
- Rapidly improving, and looking for new apps
- We can use clever tricks to check the answers!

Thank you!!