Bits vs Qubits and Quantum Advantage

CS 401: Quantum Computing
Dr. Kell, Spring 2023

High Level Review: How Classical Computers Work

(non-quantum)

Step 1: Pick the most convenient/efficient physical medium for storing and manipulating numbers.

High Level Review: How Classical Computers Work

(non-quantum)

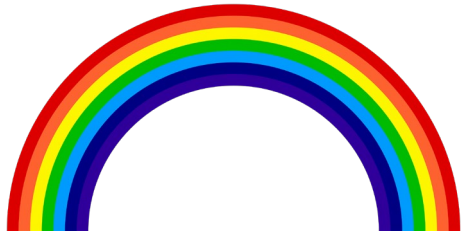
Step 1: Pick the most convenient/efficient physical medium for storing and manipulating numbers.

High Level Review: How Classical Computers Work

(non-quantum)

Step 1: Pick the most convenient/efficient physical medium for storing and manipulating numbers.

Letters/Symbols



Colors

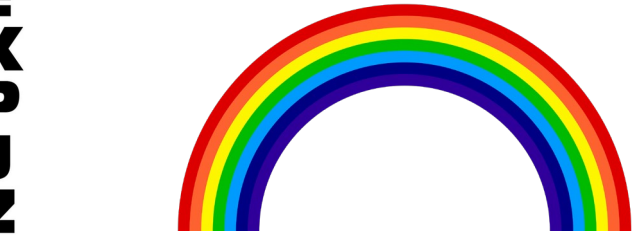
3141592653589793238462643383

Hindu-Arabic Numbers

High Level Review: How Classical Computers Work

(non-quantum)

Step 1: Pick the most convenient/efficient physical medium for storing and manipulating numbers.



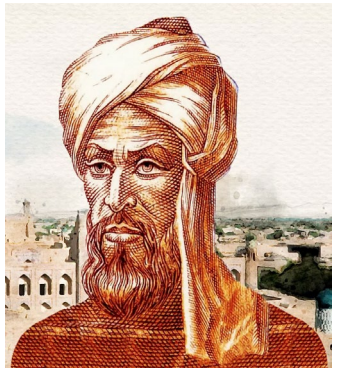
Letters/Symbols

Colors

3141592653589793238462643383

Hindu-Arabic Numbers

Invented 0-300 AD
In India



800 AD: Al Khwarizmi
(etymology of “algorithm”)
in Middle East

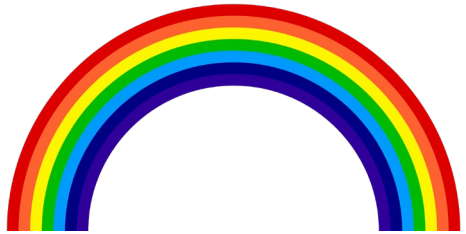
1200 AD: Fibonacci
In Europe

High Level Review: How Classical Computers Work

(non-quantum)

Step 1: Pick the most convenient/efficient physical medium for storing and manipulating numbers.

Letters/Symbols



Colors

3141592653589793238462643383

Hindu-Arabic Numbers

Binary Numbers (2 digits instead of 10)

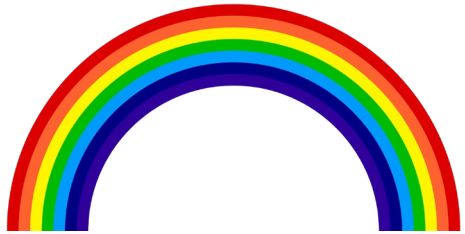
1 1 0 0 1 0 0 1

High Level Review: How Classical Computers Work

(non-quantum)

Step 1: Pick the most convenient/efficient physical medium for storing and manipulating numbers.

Letters/Symbols



Colors

3141592653589793238462643383

Hindu-Arabic Numbers

Binary Numbers (2 digits instead of 10)

1 1 0 0 1 0 0 1

Lights Switches

High Level Review: How Classical Computers Work

(non-quantum)

Step 1: Pick the most convenient/efficient physical medium for storing and manipulating numbers.

Letters/Symbols

Colors

3141592653589793238462643383

Hindu-Arabic Numbers

Binary Numbers (2 digits instead of 10)

1 1 0 0 1 0 0 1

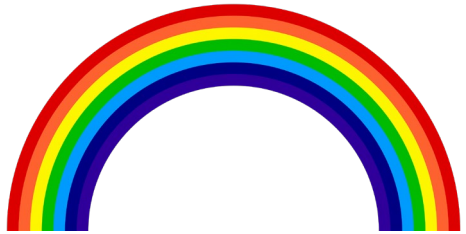
Lights Bulbs

High Level Review: How Classical Computers Work

(non-quantum)

Step 1: Pick the most convenient/efficient physical medium for storing and manipulating numbers.

Letters/Symbols



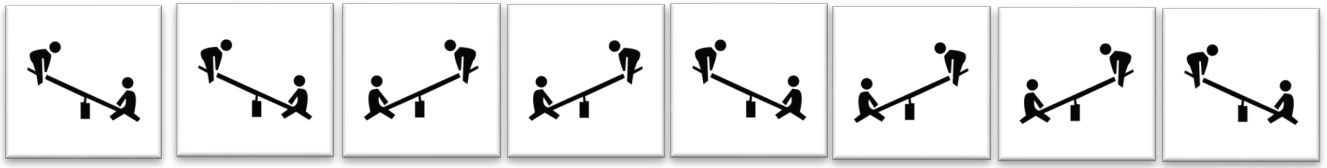
Colors

31415926535897932384626433 83

Hindu-Arabic Numbers

Binary Numbers (2 digits instead of 10)

1 1 0 0 1 0 0 1



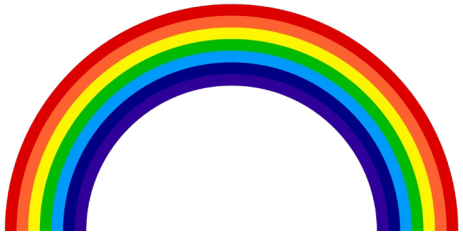
Kids on See-Saw

High Level Review: How Classical Computers Work

(non-quantum)

Step 1: Pick the most convenient/efficient physical medium for storing and manipulating numbers.

Letters/Symbols



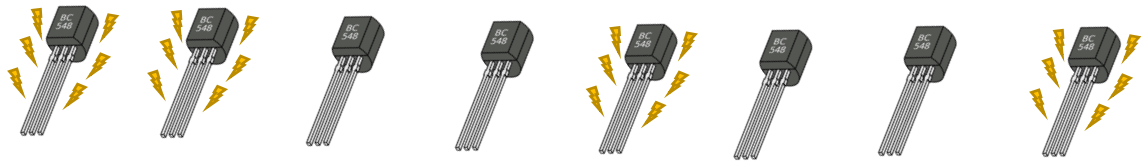
Colors

3141592653589793238462643383

Hindu-Arabic Numbers

Binary Numbers (2 digits instead of 10)

1 1 0 0 1 0 0 1



Computers Use: transistors + wires

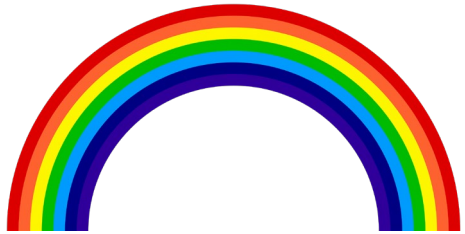
(Classical Bits of Information)

High Level Review: How Classical Computers Work

(non-quantum)

Step 1: Pick the most convenient/efficient physical medium for storing and manipulating numbers.

Letters/Symbols



Colors

3141592653589793238462643383

Hindu-Arabic Numbers

Binary Numbers (2 digits instead of 10)

1 1 0 0 1 0 0 1

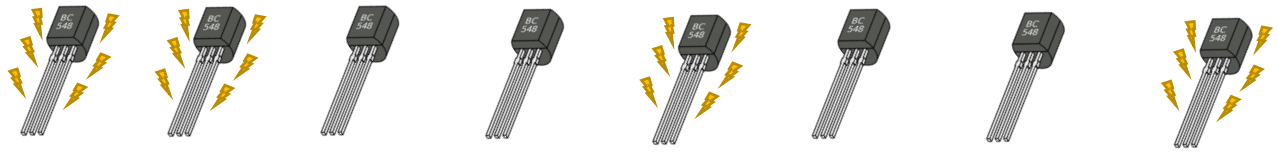
Computers Use: basically, mini light bulbs
(Classical Bits of Information)

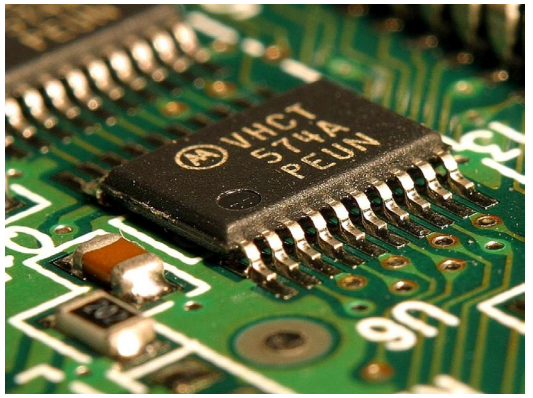
High Level Review: How Classical Computers Work

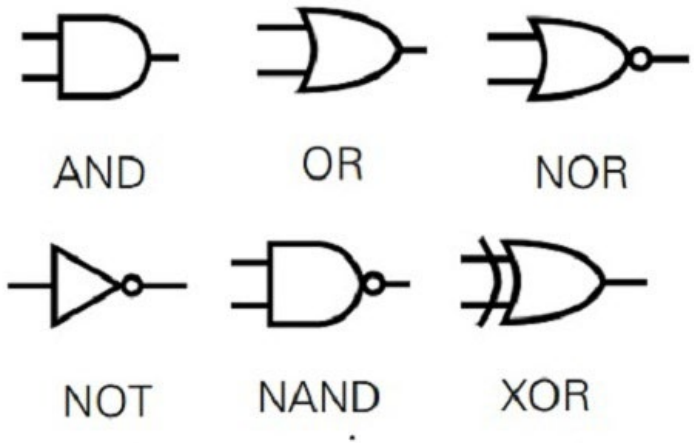
(non-quantum)

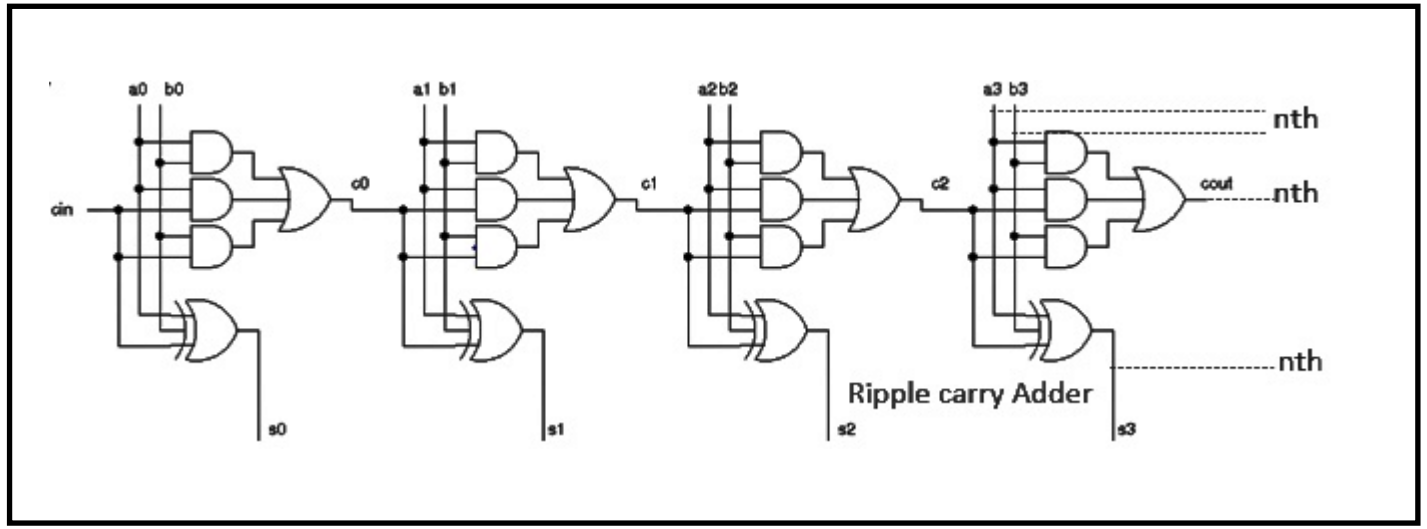
Step 2: “Automate” the process of thinking using physical information scheme.

1 1 0 0 1 0 0 1



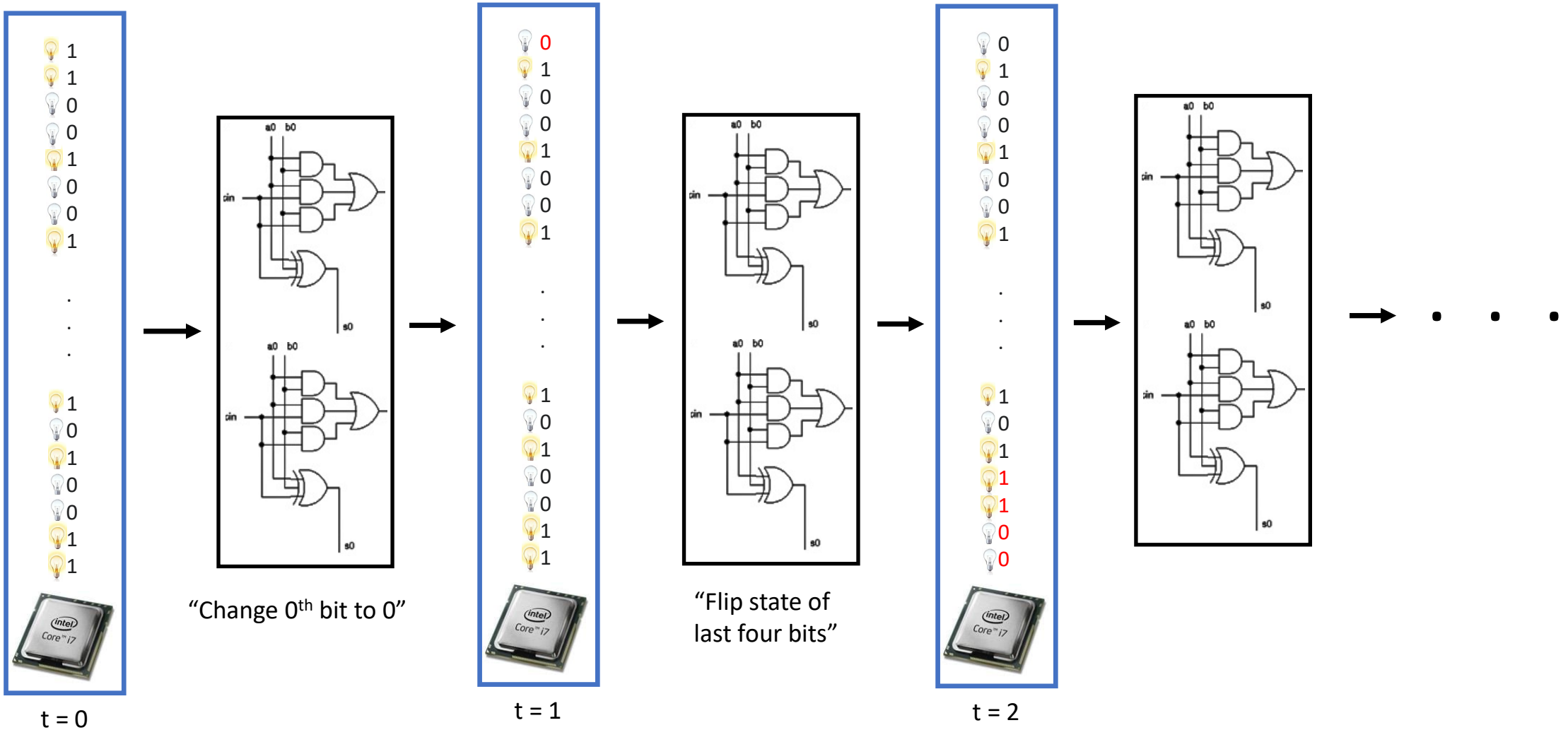






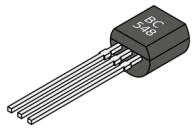
(Simplified) Evolution of Classical CPU Over Time

Entire State of CPU



Classical Bits versus Quantum Bits (“Qubits”)

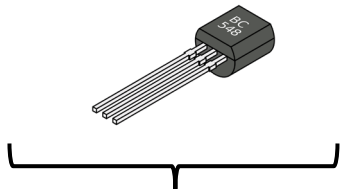
Modern Classical Bits



Transistor Size ~ 10 nanometers
(0.00000001 meters)

Classical Bits versus Quantum Bits (“Qubits”)

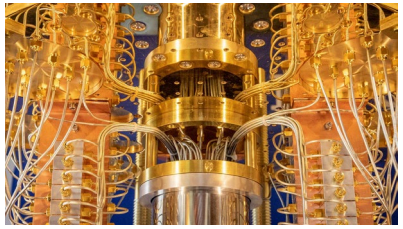
Modern Classical Bits

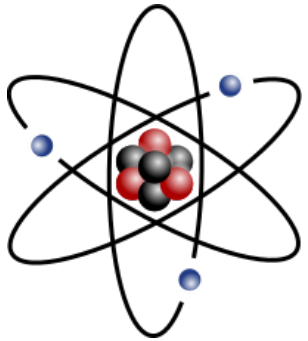


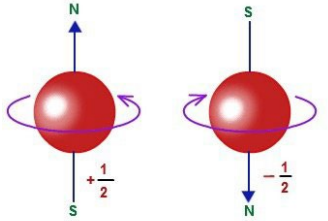
Transistor Size ~ 10 nanometers
(0.00000001 meters)

Qubit -> state of an atom or photon

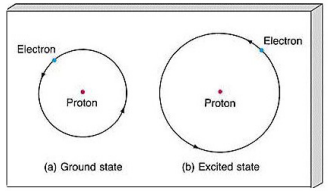
(Just make things even smaller)







“spin up” vs “spin down”



ground vs excited

Electron size ~ 10^{-18} meters
(0.000000000000000001 meters)

Canonical Problems with Quantum Advantage

Canonical Problems with Quantum Advantage

Problem 1: Factoring Integers

Input: integer x.
Output: non-trivial factors of x.

x = 54 ⟶ 2, 3, 6, 9, 18, 27

Best Classical Algorithm: O(2^n) for n bit numbers

Shor's Quantum Algorithm: O(poly(n))

Many cryptography schemes (e.g., RSA) rely on exponential runtime for the problem.

Canonical Problems with Quantum Advantage

Problem 1: Factoring Integers

Input: integer x.
Output: non-trivial factors of x.

x = 54 ⟶ 2, 3, 6, 9, 18, 27

Best Classical Algorithm: O(2^n) for n bit numbers

Shor's Quantum Algorithm: O(poly(n))

Many cryptography schemes (e.g., RSA) rely on exponential runtime for the problem.

Problem 2: Search Problem

Input: list L, target value
Output: index of target in L

L = [2, 1, 10, 4, 7, 9, 3]
target = 7
⟶ 4 (index of 7)

Many applications in cloud quantum computing, databases, etc.

Canonical Problems with Quantum Advantage

Problem 1: Factoring Integers

Input: integer x.
Output: non-trivial factors of x.

x = 54 ⟶ 2, 3, 6, 9, 18, 27

Best Classical Algorithm: O(2^n) for n bit numbers

Shor's Quantum Algorithm: O(poly(n))

Many cryptography schemes (e.g., RSA) rely on exponential runtime for the problem.

Problem 2: Search Problem

Input: list L, target value
Output: index of target in L

L = [2, 1, 10, 4, 7, 9, 3]
target = 7
⟶ 4 (index of 7)

Many applications in cloud quantum computing, databases, etc.

Best Possible Classical Algorithm: O(n)

Canonical Problems with Quantum Advantage

Problem 1: Factoring Integers

Input: integer x.
Output: non-trivial factors of x.

x = 54 ⟶ 2, 3, 6, 9, 18, 27

Best Classical Algorithm: O(2^n) for n bit numbers

Shor's Quantum Algorithm: O(poly(n))

Many cryptography schemes (e.g., RSA) rely on exponential runtime for the problem.

Problem 2: Search Problem

Input: list L, target value
Output: index of target in L

L = [2, 1, 10, 4, 7, 9, 3]
target = 7
⟶ 4 (index of 7)

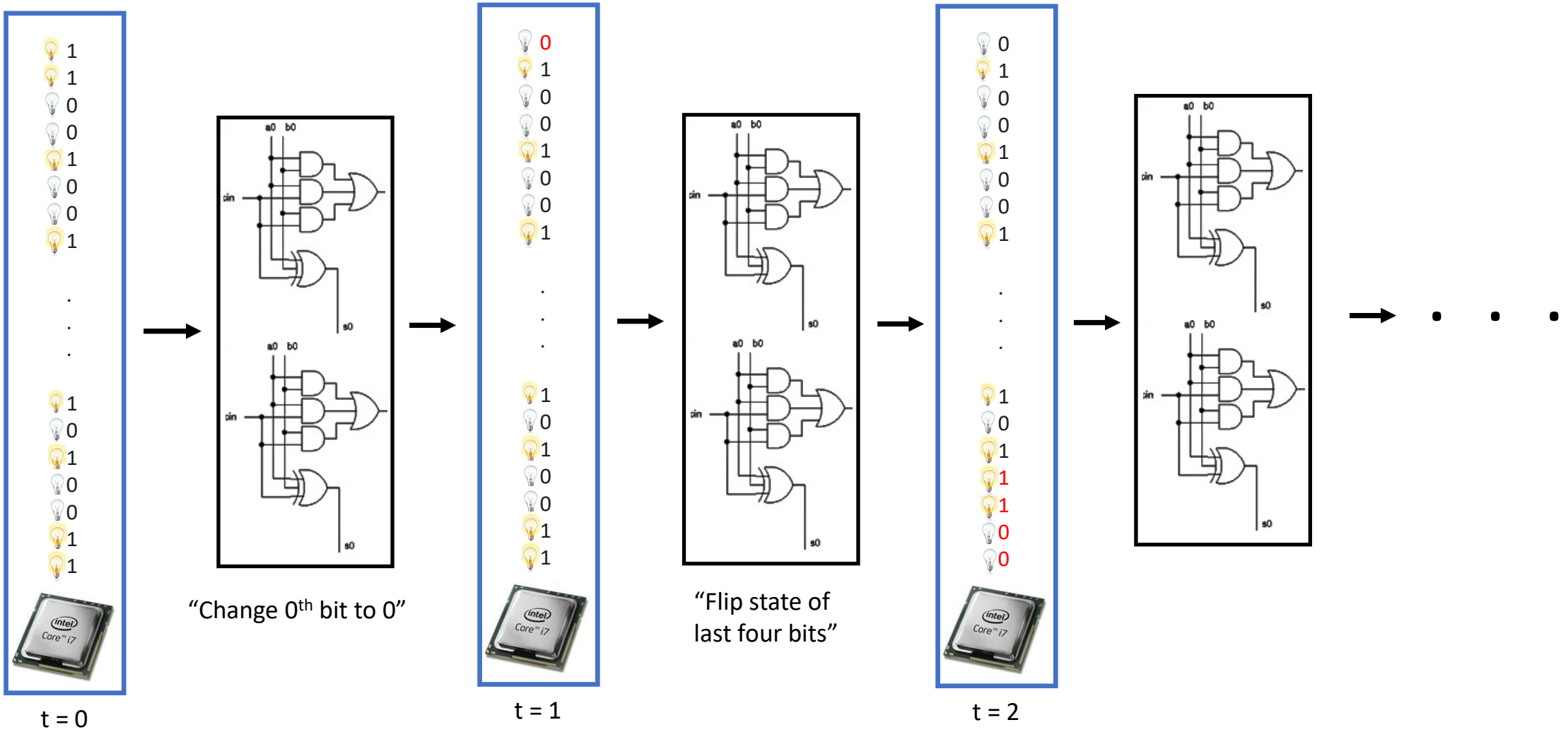
Many applications in cloud quantum computing, databases, etc.

Best Possible Classical Algorithm: O(n)

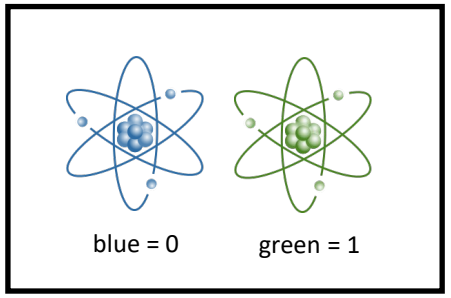
Grover's Quantum Algorithm: O($n^{1/2}$)

High Level: Why is this possible?

Entire State of CPU

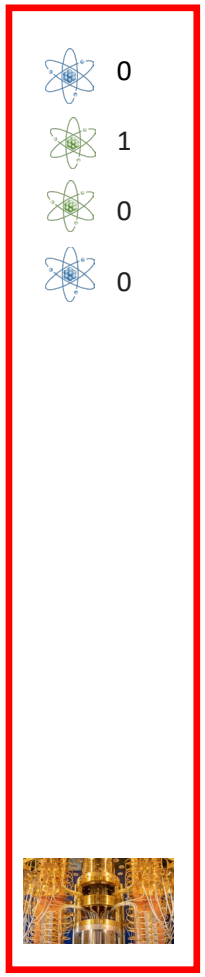


High Level: Why is this possible?

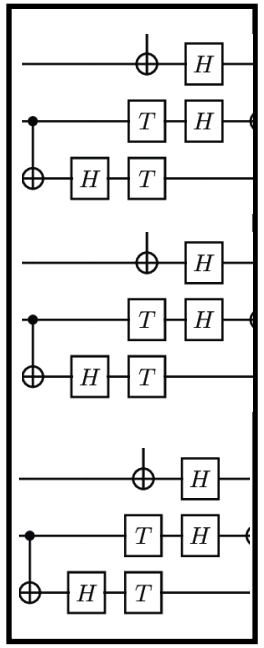


Qubit = some property of atom

State Quantum CPU

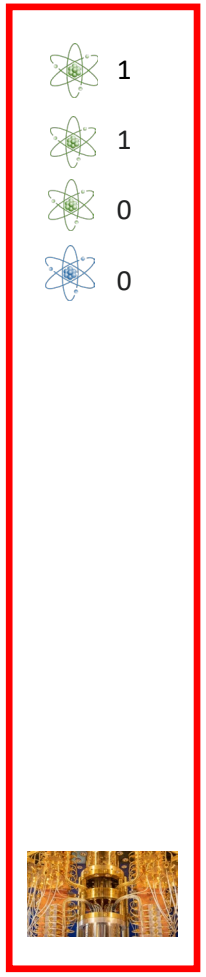


t = 0

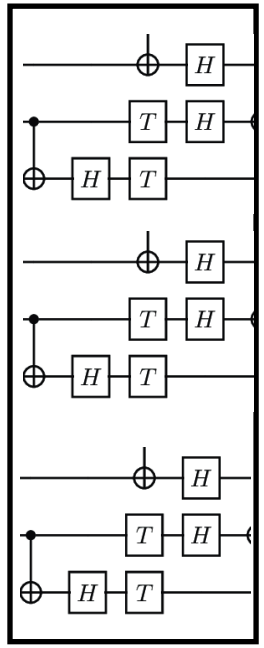


Quantum Logic Gates

State Quantum CPU

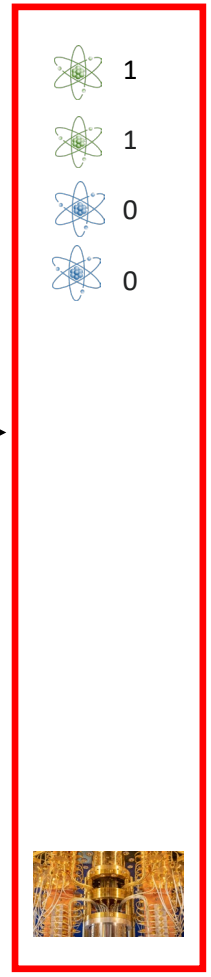


t = 1

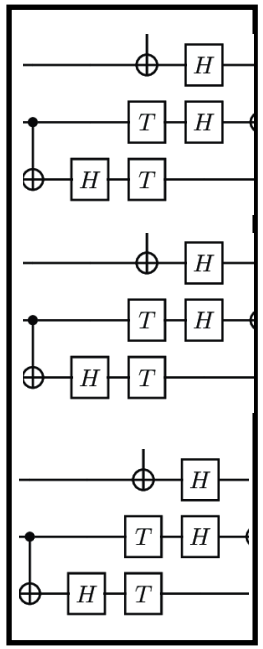


Quantum Logic Gates

State Quantum CPU



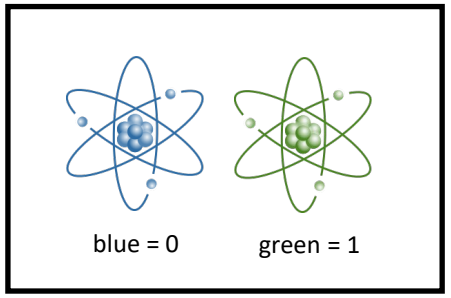
t = 2



Quantum Logic Gates

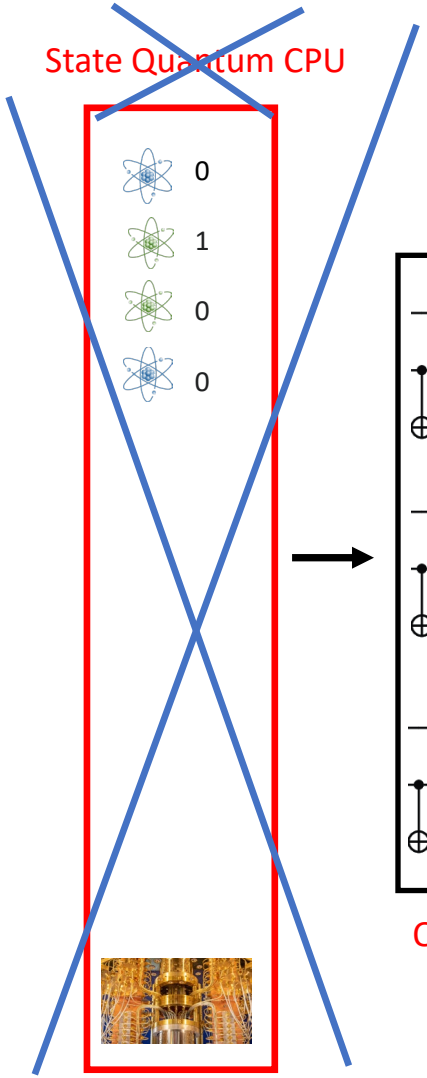
. . .

High Level: Why is this possible?

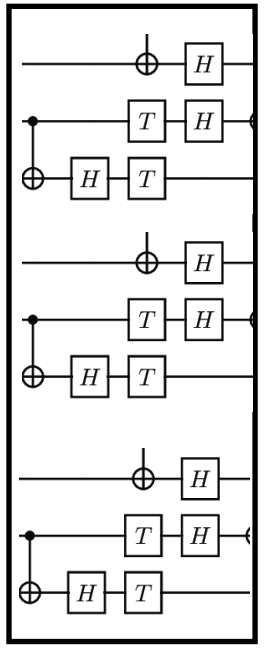


Qubit = some property of atom

State Quantum CPU

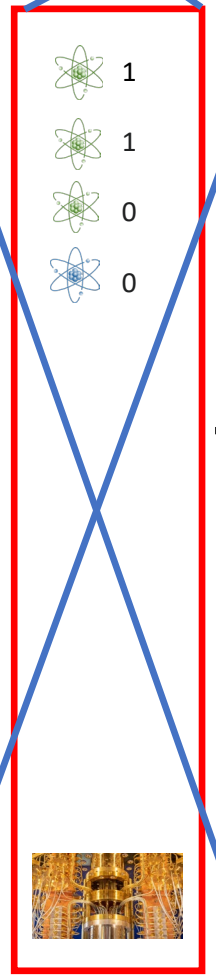


t = 0

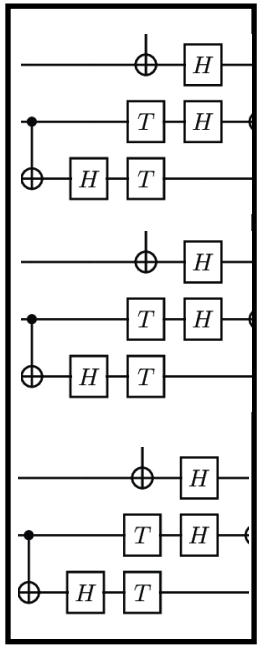


Quantum Logic Gates

State Quantum CPU

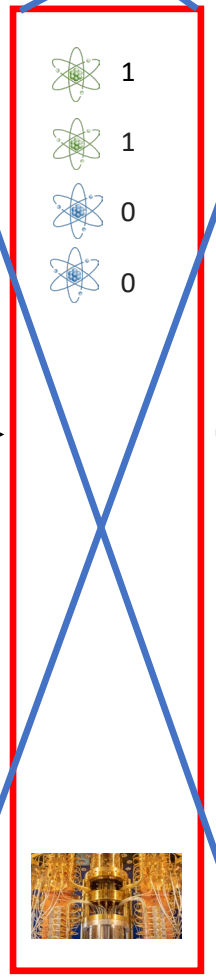


t = 1

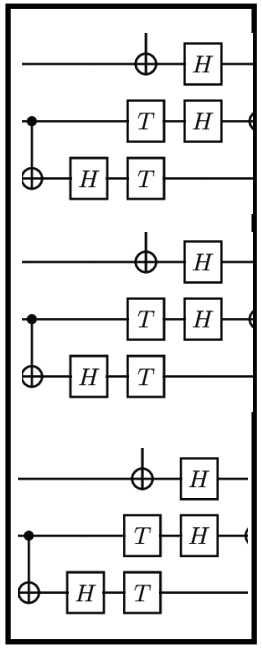


Quantum Logic Gates

State Quantum CPU



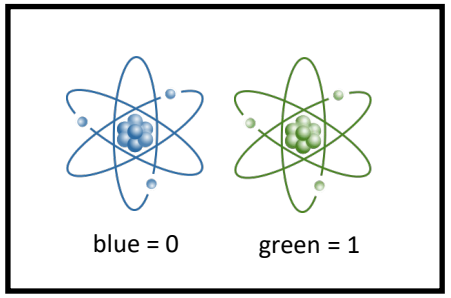
t = 2



Quantum Logic Gates

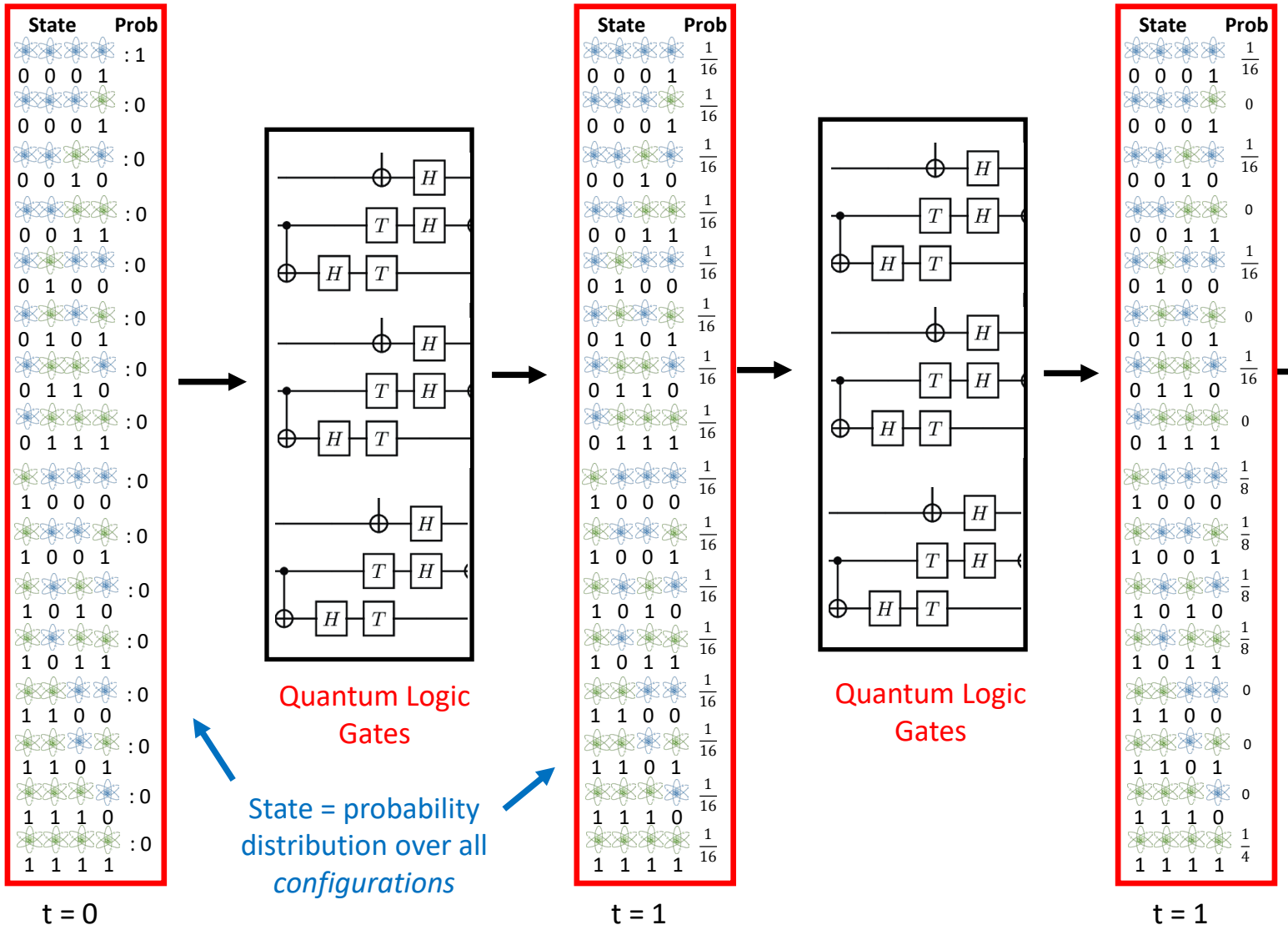
. . .

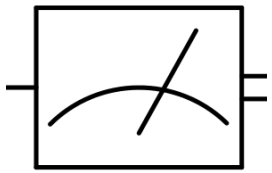
High Level: Why is this possible?



Qubit = some property of atom

State Quantum CPU





Measure/Observe

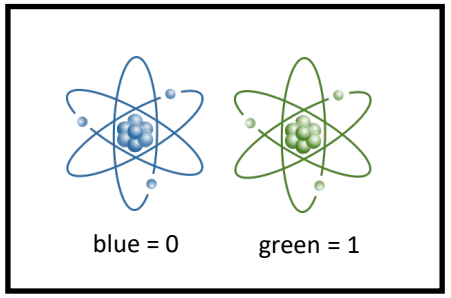
(Picks state according to probabilities)

Single outcome

1 0 1 0

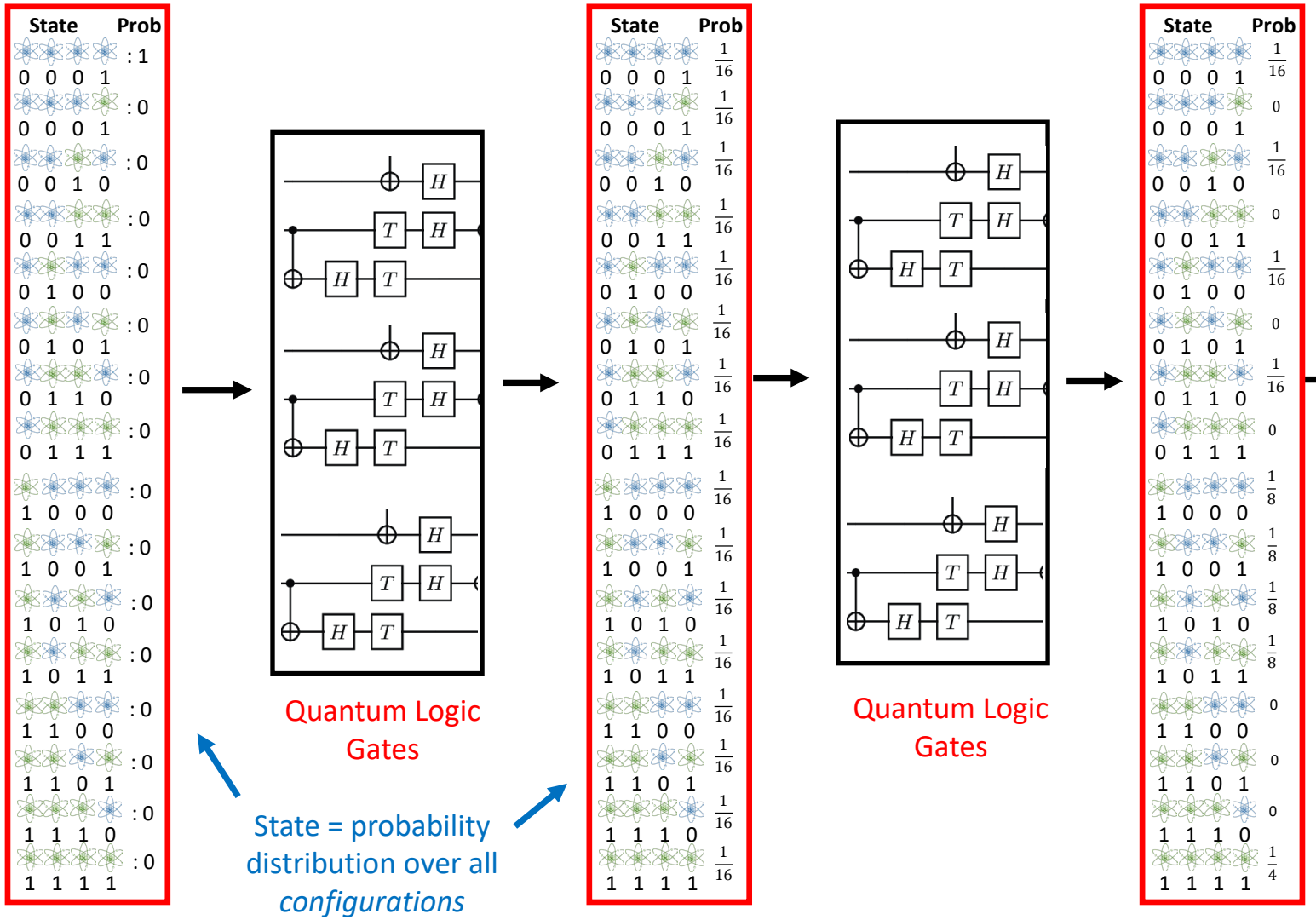
(had 1/8 chance)

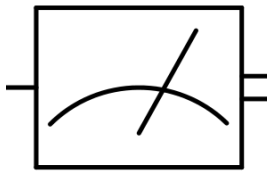
High Level: Why is this possible?



Qubit = some property of atom

State Quantum CPU





Measure/Observe

(Picks state according to probabilities)

Single outcome

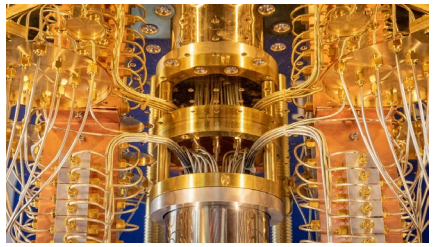
1 0 1 0

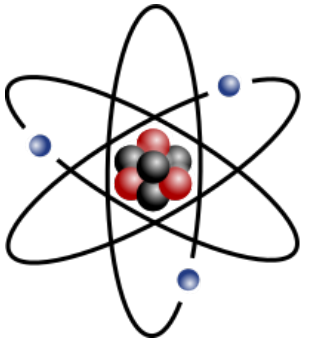
(had 1/8 chance)

… Well, not exactly

- Probabilities can actually be *negative* or *complex* numbers.
- What happens if we measure some atoms/qubits but not others?

Conclusions

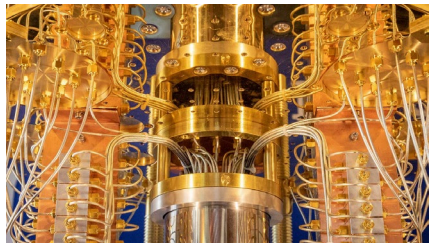


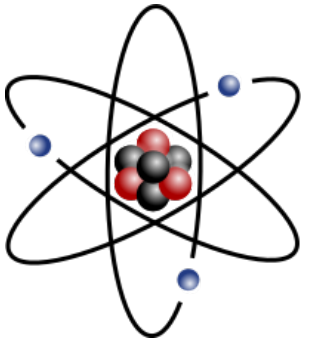


Key Takeaways

- **Quantum computers can be faster** because they get to manipulate and exponential amount of information in O(1) time.
- **Quantum computers are not 100%** superior nor solve all hard problems trivially because:
    - The rules for how exponential probabilities are updated are constrained to certain operations.
    - Even though we get to manipulate an exponential number of probabilities, we only see one outcome at the end.

Conclusions



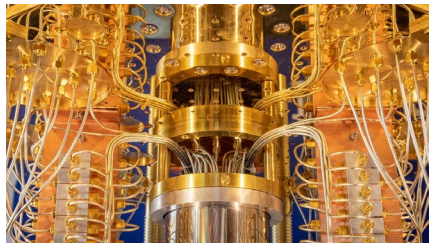


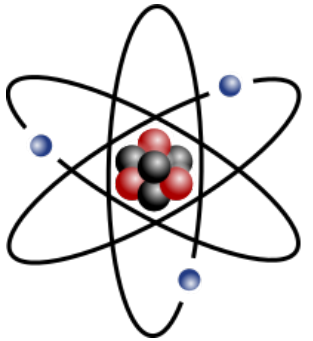
Key Takeaways

- **Quantum computers can be faster** because they get to manipulate and exponential amount of information in O(1) time.
- **Quantum computers are not 100%** superior nor solve all hard problems trivially because:
    - The rules for how exponential probabilities are updated are constrained to certain operations.
    - Even though we get to manipulate an exponential number of probabilities, we only see one outcome at the end.

Question: How does “Nature” keep track of and update so much information so quickly?

Conclusions





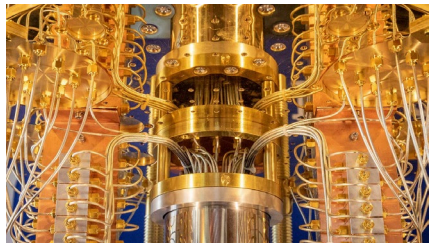
Key Takeaways

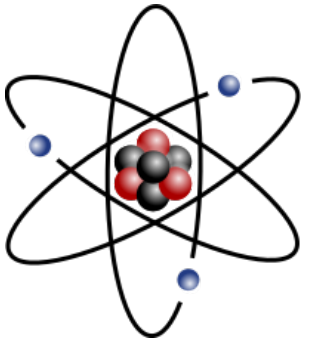
- **Quantum computers can be faster** because they get to manipulate and exponential amount of information in O(1) time.
- **Quantum computers are not 100%** superior nor solve all hard problems trivially because:
    - The rules for how exponential probabilities are updated are constrained to certain operations.
    - Even though we get to manipulate an exponential number of probabilities, we only see one outcome at the end.

Question: How does “Nature” keep track of and update so much information so quickly?

- **Answer:**

Conclusions





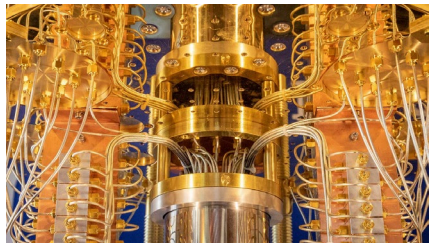
Key Takeaways

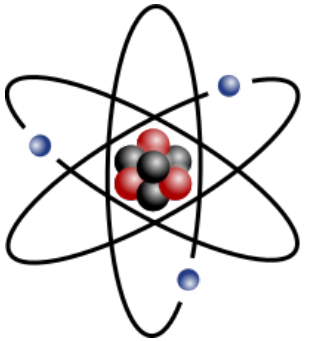
- **Quantum computers can be faster** because they get to manipulate and exponential amount of information in O(1) time.
- **Quantum computers are not 100%** superior nor solve all hard problems trivially because:
    - The rules for how exponential probabilities are updated are constrained to certain operations.
    - Even though we get to manipulate an exponential number of probabilities, we only see one outcome at the end.

Question: How does “Nature” keep track of and update so much information so quickly?

- **Answer:** Nobody knows.

Conclusions





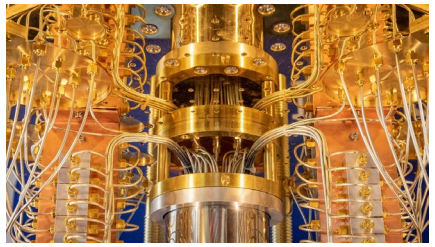
Key Takeaways

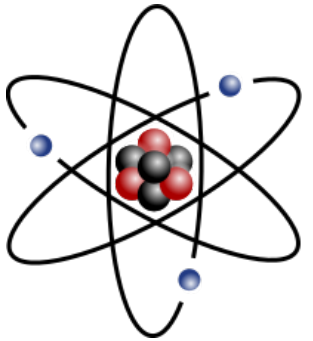
- **Quantum computers can be faster** because they get to manipulate and exponential amount of information in O(1) time.
- **Quantum computers are not 100%** superior nor solve all hard problems trivially because:
    - The rules for how exponential probabilities are updated are constrained to certain operations.
    - Even though we get to manipulate an exponential number of probabilities, we only see one outcome at the end.

Question: How does “Nature” keep track of and update so much information so quickly?

- **Answer:** Nobody knows.
- Three categories/types of answers:

Conclusions





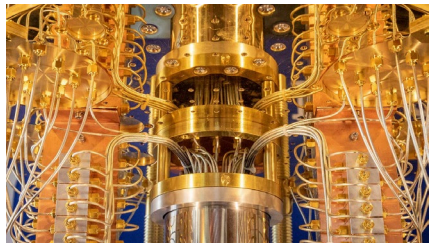
Key Takeaways

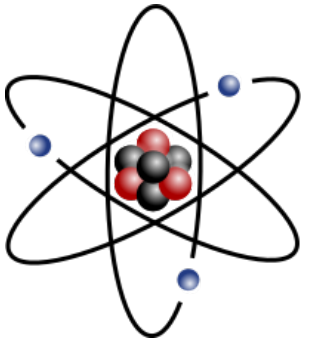
- **Quantum computers can be faster** because they get to manipulate and exponential amount of information in O(1) time.
- **Quantum computers are not 100%** superior nor solve all hard problems trivially because:
    - The rules for how exponential probabilities are updated are constrained to certain operations.
    - Even though we get to manipulate an exponential number of probabilities, we only see one outcome at the end.

Question: How does “Nature” keep track of and update so much information so quickly?

- **Answer:** Nobody knows.
- Three categories/types of answers:
    1. **Who cares? Quantum physics works why ask the question?**

Conclusions





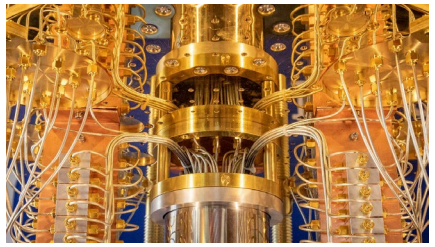
Key Takeaways

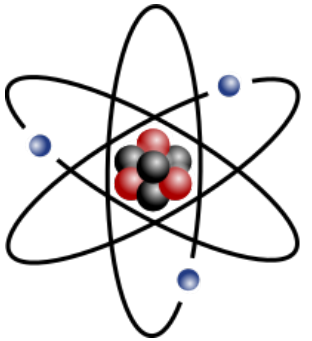
- **Quantum computers can be faster** because they get to manipulate and exponential amount of information in O(1) time.
- **Quantum computers are not 100%** superior nor solve all hard problems trivially because:
    - The rules for how exponential probabilities are updated are constrained to certain operations.
    - Even though we get to manipulate an exponential number of probabilities, we only see one outcome at the end.

Question: How does “Nature” keep track of and update so much information so quickly?

- **Answer:** Nobody knows.
- Three categories/types of answers:
    1. Who cares? Quantum physics works why ask the question?
    2. Quantum mechanics doesn’t make sense, thus needs fixed.

Conclusions





Key Takeaways

- **Quantum computers can be faster** because they get to manipulate and exponential amount of information in O(1) time.
- **Quantum computers are not 100%** superior nor solve all hard problems trivially because:
  - The rules for how exponential probabilities are updated are constrained to certain operations.
  - Even though we get to manipulate an exponential number of probabilities, we only see one outcome at the end.

Question: How does “Nature” keep track of and update so much information so quickly?

- **Answer:** Nobody knows.
- Three categories/types of answers:
  1. Who cares? Quantum physics works why ask the question?
  2. Quantum mechanics doesn’t make sense, thus needs fixed.
  3. We live in a multiverse which interact *(many-worlds interpretation).*