

# THE STORY OF QUANTUM COMPUTING

By

Aitanjali Venkataraman

# FOREWORD

The book you're holding contains the basics of quantum computing in the form of a comic book. It's charming and delightful and awesome. The author, Gitanjali Venkatraman, contacted me more-or-less out of the blue with a draft of the book. I wasn't sure what to expect, but I was blown away by the craftsmanship that went into the book -- especially the beautiful illustrations on every page (the minimalist caricatures of my colleagues never failed to make me smile).

For a quarter of a century, most popularizations of quantum computing have tried to take the easy way out: a qubit is just a bit that's 0 and 1 at the same time, and a quantum computer solves hard problems in an instant by trying every possible answer in parallel. The problem with these pat answers is twofold. First, they miss the real beauty of quantum information -- a beauty that has to do with amplitudes, square roots of probabilities (!), interfering and canceling each other out, to kill off the wrong answers to a problem and leave only the right answers -- an effect weird enough that I doubt any science fiction writer would ever have had the imagination to invent it. Second, I've seen again and again how the pat answers fill people with ideas of what quantum computers will be able to do in practice that are wildly off, leaving them vulnerable to snake-oil salesmen.

Even though it's written for a broad audience, this book makes a genuine effort to avoid the temptations of falsehood and grapple with the richness of the field. I hope you enjoy it as much as I did.

Scott Aaronson
Austin, TX
August 2020

# INTRODUCTION

AT THE SMALLEST SCALES IN THE UNIVERSE, AT THE LEVEL OF AN ATOM, THE LAWS OF PHYSICS ARE WEIRD. WE CAN PRECISELY KNOW WHERE AN ELECTRON IS, BUT NOT HOW FAST IT MOVES. AS FOR WHERE, AN ELECTRON COULD BE IN MANY PLACES AT ONCE. DESCRIBING THESE IS THE JOB OF QUANTUM PHYSICS.

QUANTUM PHYSICS TOGETHER WITH COMPUTER SCIENCE MAKE A NEW TYPE OF COMPUTER CALLED THE QUANTUM COMPUTER. IT USES THE WEIRDNESS OF THE QUANTUM WORLD TO SOLVE PROBLEMS WE MIGHT NOT BE ABLE TO SOLVE WITH SUPERCOMPUTERS.

IT COULD CRACK CODES FASTER THAN SUPERCOMPUTERS, HELP US BUILD BETTER DRUGS AND MATERIALS ALL WITH THE TANTALISING PROMISE OF EXTRAORDINARY SPEED.

WHY ARE SOME PROBLEMS HARDER TO SOLVE THAN OTHERS? WHO THOUGHT OF MAKING A QUANTUM COMPUTER? HOW DIFFERENT ARE THEY TO THE ONES WE USE NOW? ARE THERE THINGS IT CANNOT DO?

TAKE A VISUAL TOUR OF ITS EVOLUTION: THE PEOPLE, THE PHYSICS AND A FLAVOUR OF HOW WE MIGHT PROGRAM IT. THIS IS A FULLY ILLUSTRATED GUIDE.

THIS IS THE STORY OF QUANTUM COMPUTING.

# ACKNOWLEDGEMENTS


THIS BOOK IS POSSIBLE ONLY BECAUSE OF THE SEVERAL INFLUENCES IN MY LIFE

FIRSTLY, MY GRATEFUL THANKS TO SCOTT AARONSON, DIRECTOR OF THE QUANTUM INFORMATION CENTRE AT THE UNIVERSITY OF TEXAS AUSTIN, FOR RESPONDING TO MY EMAIL AND FOR TAKING TIME TO GIVE VALUABLE INPUTS TO MY DRAFT AND FOR HIS VERY ENCOURAGING WORDS.

MANY THANKS TO REBECCA PARSONS, CTO-THOUGHTWORKS, FOR HER UNQUESTIONING SUPPORT OF MY WORK AND TO MY COLLEAGUES WITH WHO I HAVE EXCHANGED IDEAS.

MY GRATITUDE TO

DAVE ELLIMAN FOR BELIEVING I COULD

JAYNE EVANS MY ART TEACHER

MY BOYS & ASHOK FOR BEING THERE

MY MOTHER, FOR EVERYTHING

# CONTENTS


WHAT IS A QUANTUM COMPUTER? — 1

WHY MIGHT WE NEED ONE? — 2

END OF MOORE'S LAW? — 3

A TOUR OF COMPUTATIONAL COMPLEXITY — 4

ALL ABOUT QUANTUM — 21

QUANTUM VS CLASSICAL — 23

PARTICLES AND WAVES — 24

BEGINNING OF QUANTUM THEORY — 26

QUANTUM WEIRDNESS — 32

SUPERPOSITION — 33

ENTANLEMENT — 36

REACTIONS TO QUANTUM MECHANICS — 39

APPLICATIONS OF QUANTUM MECHANICS — 40

QUANTUM COMPUTERS: A NEW IDEA — 41

HARDWARE OVERVIEW & CHALLENGES — 42

THE EXPONENTIAL POWER OF QUANTUM — 44

QUANTUM BITS — 47

BITS, QUBITS, STATES — 49

MATHEMATICAL MODEL OF QUBITS — 51

WAVES, AMPLITUDES & MEASUREMENT — 54

LOGIC GATES — 61

A FEW BASIC QUANTUM LOGIC GATES — 63

GATES & ENTANGLEMENT — 68

QUANTUM ALGORITHMS — 71

DEUTSCH-JOZSA — 74

GROVER ALGORITHM — 82

SHOR'S ALGORITHM — 88

QUANTUM COMPUTERS SOLVE EVERYTHING? — 96

DO AND NOT DO — 98

ALGORITHM EFFICIENCY — 99

A NEW COMPLEXITY CLASS — 100

SECURITY AND QUANTUM COMPUTERS — 101

BREAKING CRYPTO — 102

QUANTUM-SAFE CRYPTO — 103

QUANTUM KEY DISTRIBUTION — 104

ERROR CORRECTION — 106

PROGRAMMING AND TESTING — 110

PRESENT AND FUTURE — 112

WOMEN IN QUANTUM COMPUTING — 116

REFERENCES — 121

# WHAT IS A QUANTUM COMPUTER?

SO WHAT IS A ...
..QUANTUM COMPUTER?



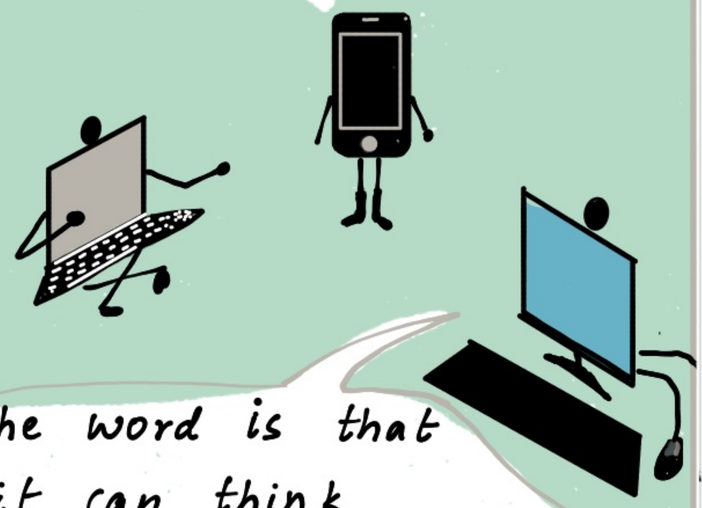
It is a computer built using QUANTUM PHYSICS

AREN'T ALL COMPUTERS BUILT ON PHYSICS? WHY IS QUANTUM ANY DIFFERENT?



yes, long story though..

IS IT CLEVERER THAN ALL OF US? OR FASTER?



The word is that it can think a trillion thoughts at once

It lives in the coldest climes. It is both fragile and sharp...



and capable of solving the hardest of problems

IS IT BETTER AT PLAYING MUSIC, SHOPPING, TELLING THE WAY, MAKING A GRAPH?



Of course not!

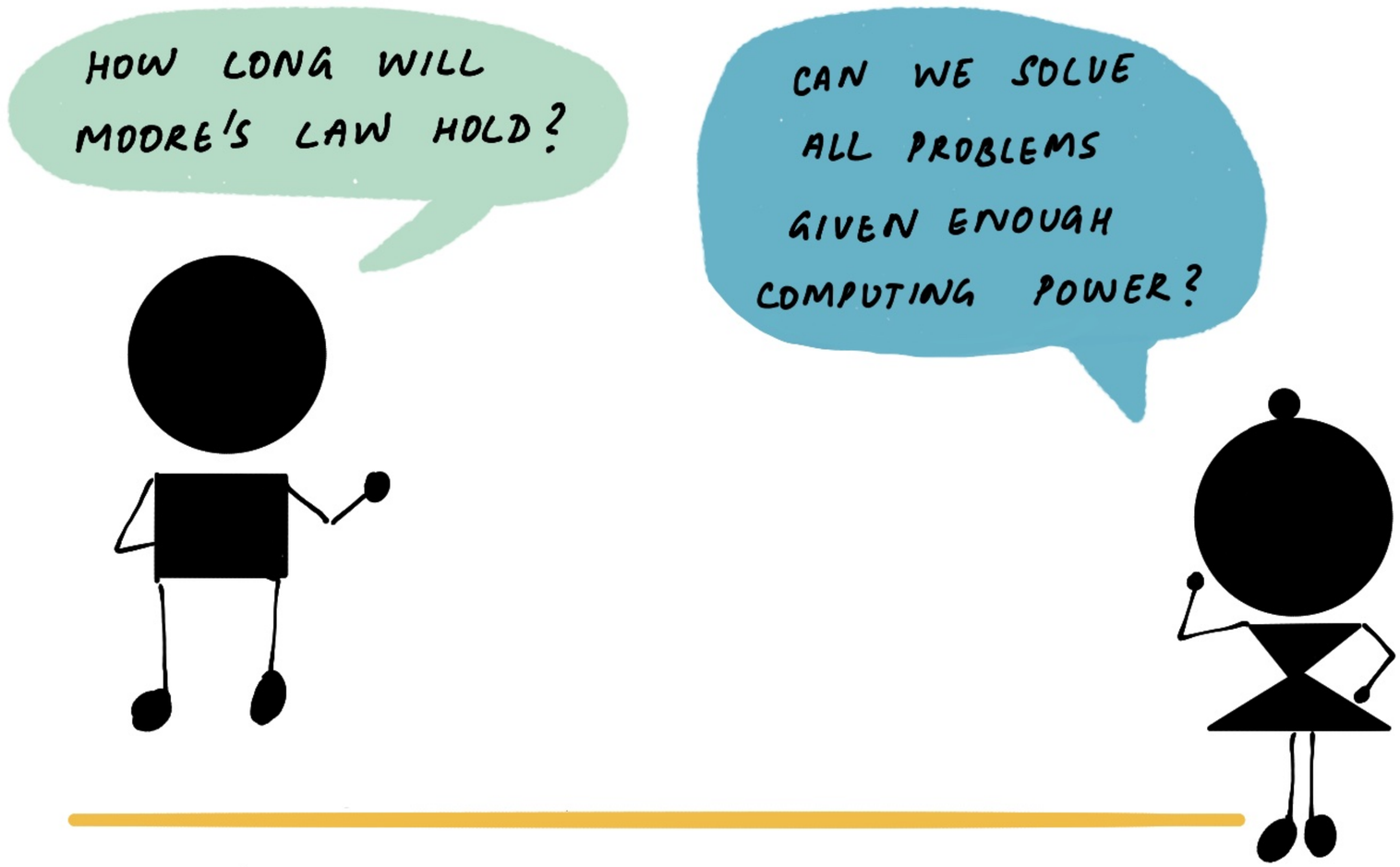
DOES IT EXIST?



Yes, but....

# DO WE NEED QUANTUM COMPUTERS

NOT SO MUCH NEED AS IT MAY BE INEVITABLE
ESPECIALLY IN LIGHT OF THESE QUESTIONS




ALSO, QUANTUM COMPUTERS ARE NOT INTENDED
AS A REPLACEMENT TO THE ONES WE NOW USE

# END OF MOORE'S LAW?

## THE "LAW"

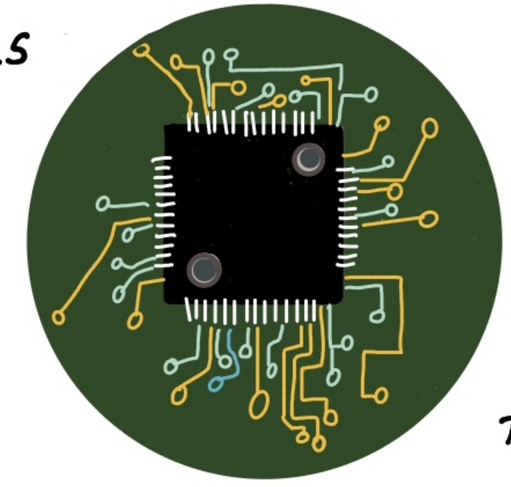


we can expect the speed of computers to double every 2 years or so

GORDON MOORE
1965

## THE PROCESSOR

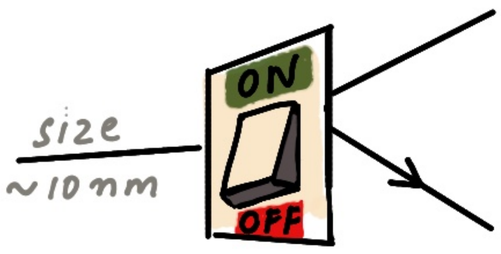
PROCESSORS HAVE BECOME CHEAPER + SMALLER



ONE CHIP CONTAINS ABOUT A BILLION TRANSISTORS

## THE TRANSISTOR

TRANSISTOR IS THE SIMPLEST PROCESSOR

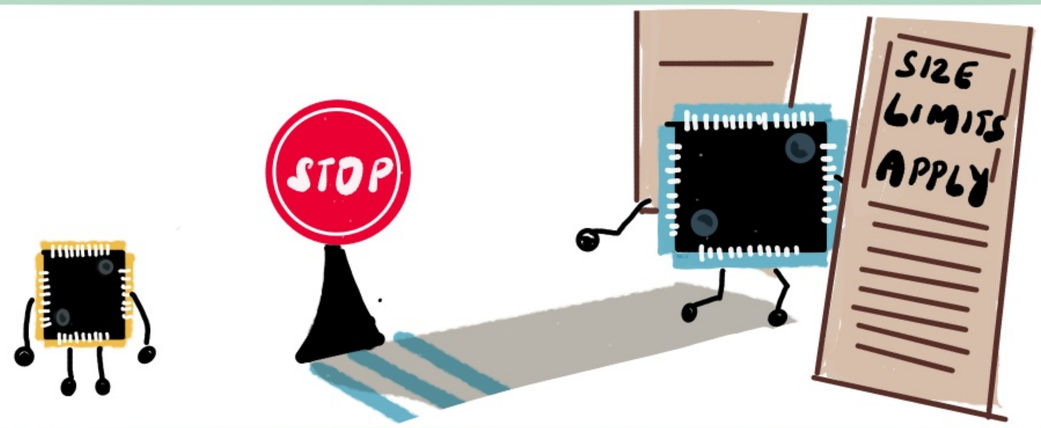



IT IS A SWITCH TO LET ELECTRONS FLOW - OR NOT

MUCH SMALLER THAN HUMAN HAIR

## THE END?

AS THE TRANSISTOR SIZE GETS SMALLER...




...QUANTUM EFFECTS* WILL COME INTO PLAY

*QUANTUM TUNNELING - WILL MAKE ELECTRONS 'JUMP' AND FLOW EVEN WHEN THE SWITCH IS 'OFF'

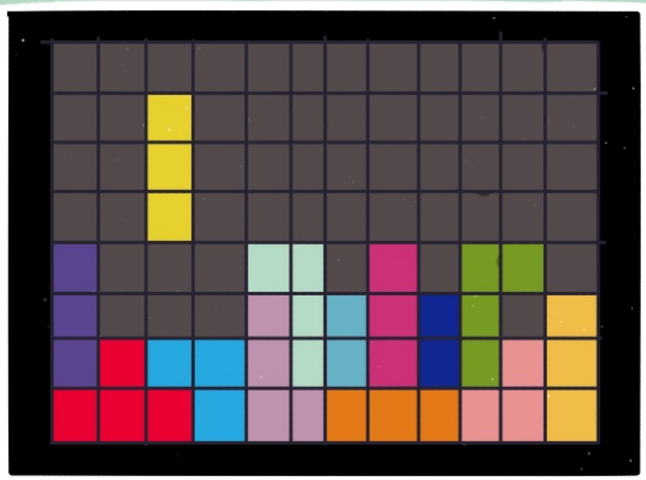
# PROBLEMS : DIFFICULT OR NOT?

## ANSWER A RIDDLE

If you have me
you want to share me
If you share me
you lose me
WHAT AM I?

answer: SECRET

## PLAY TETRIS



## SOLVE NUMBER PROBLEMS




## WIN AT CHESS



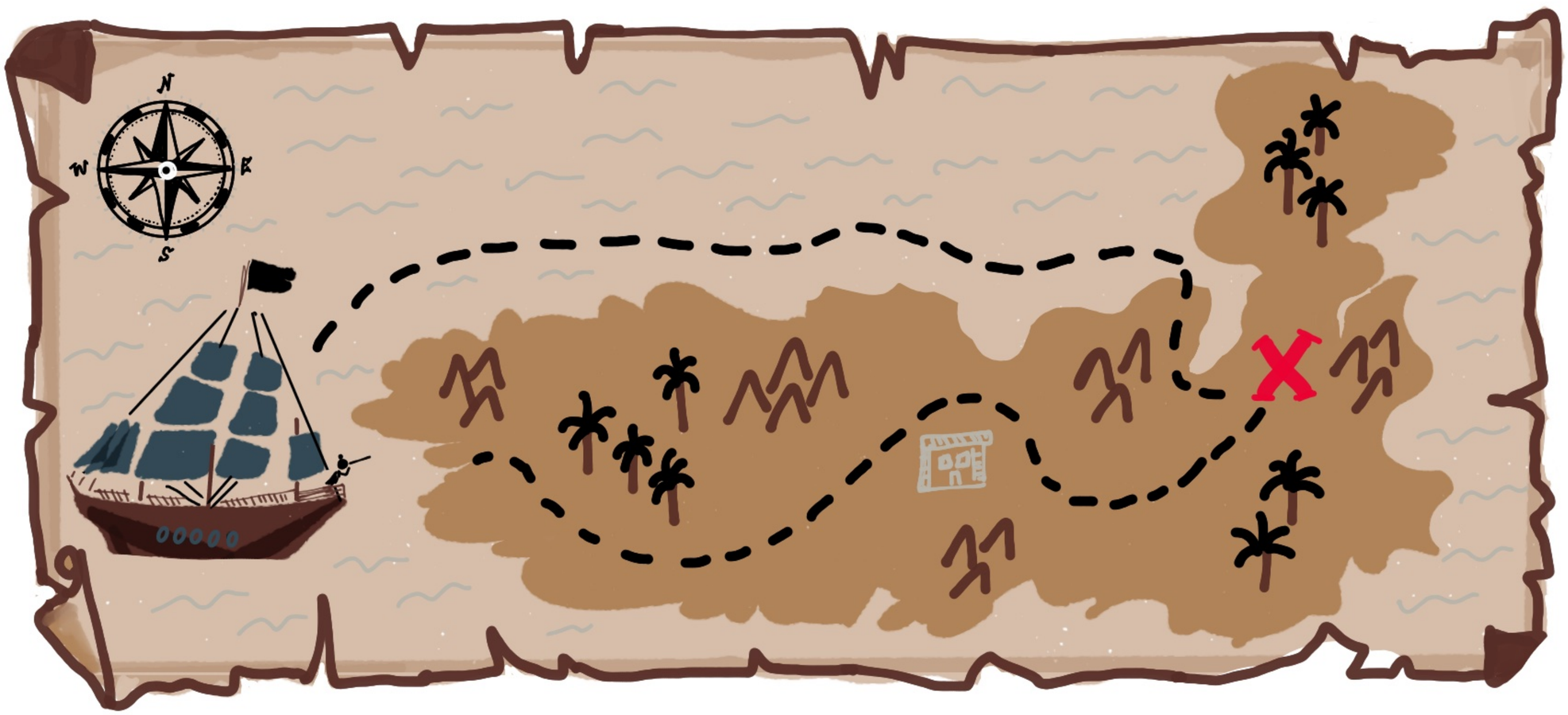
## SOLVE A SUDOKU

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | 7 | 5 | | |
| 7 | | | 1 | | | | 4 | |
| 5 | | | | | | 2 | | |
| | | | 3 | 9 | | | | 8 |
| 3 | | | 7 | 8 | 6 | | | 4 |
| 8 | | | | 4 | 1 | 7 | | |
| | | 8 | | | | | | 9 |
| | 5 | | | | 3 | | | 1 |
| | | 4 | 6 | | | | | |

## COUNT GRAINS OF SAND



# TO GET TO A SOLUTION




WITH COMPUTERS

DOES A SOLUTION EXIST?

IS THERE A SOLUTION?

AN ALGORITHM?

WITH COMPUTERS

HOW MANY STEPS?

HOW LONG DOES IT TAKE?

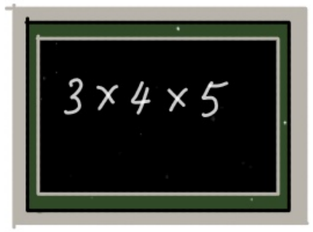
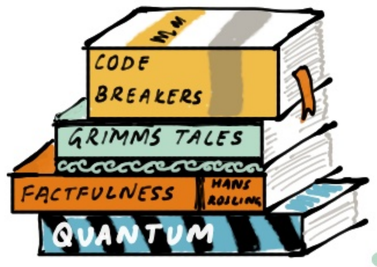
AND HOW MUCH OF THE RESOURCES?

DOES THE PROGRAM EVENTUALLY STOP?

IS THE SOLUTION EFFICIENT?

# DIFFICULTY OF TOO MANY STEPS




| TASK | | HOW MANY ADDITIONAL STEPS? |
|---|---|---|
| BAKE A CAKE<br>GIVEN INGREDIENTS |  | GIVEN INGREDIENTS X 12 |
| MULTIPLY NUMBERS<br>GIVEN 3 NUMBERS |  | GIVEN 100 NUMBERS |
| SORT BOOKS BY TITLE<br>GIVEN A PILE OF BOOKS |  | GIVEN A LIBRARY OF BOOKS |
| SOLVE A RUBIK'S CUBE<br>GIVEN A 2X2 CUBE |  | GIVEN AN 8X8 CUBE |

DIFFICULT

# ON SOLVING PROBLEMS

# DIFFICULTY WITH TRIAL & ERROR

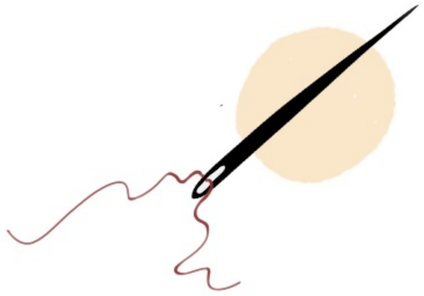


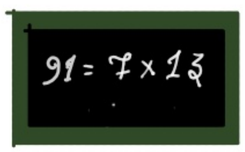

PROBLEM

FIND A NEEDLE IN A BOX

FIND PRIME FACTORS OF 91

FIND A 3-LETTER PATTERN IN A VERY LONG SEQUENCE









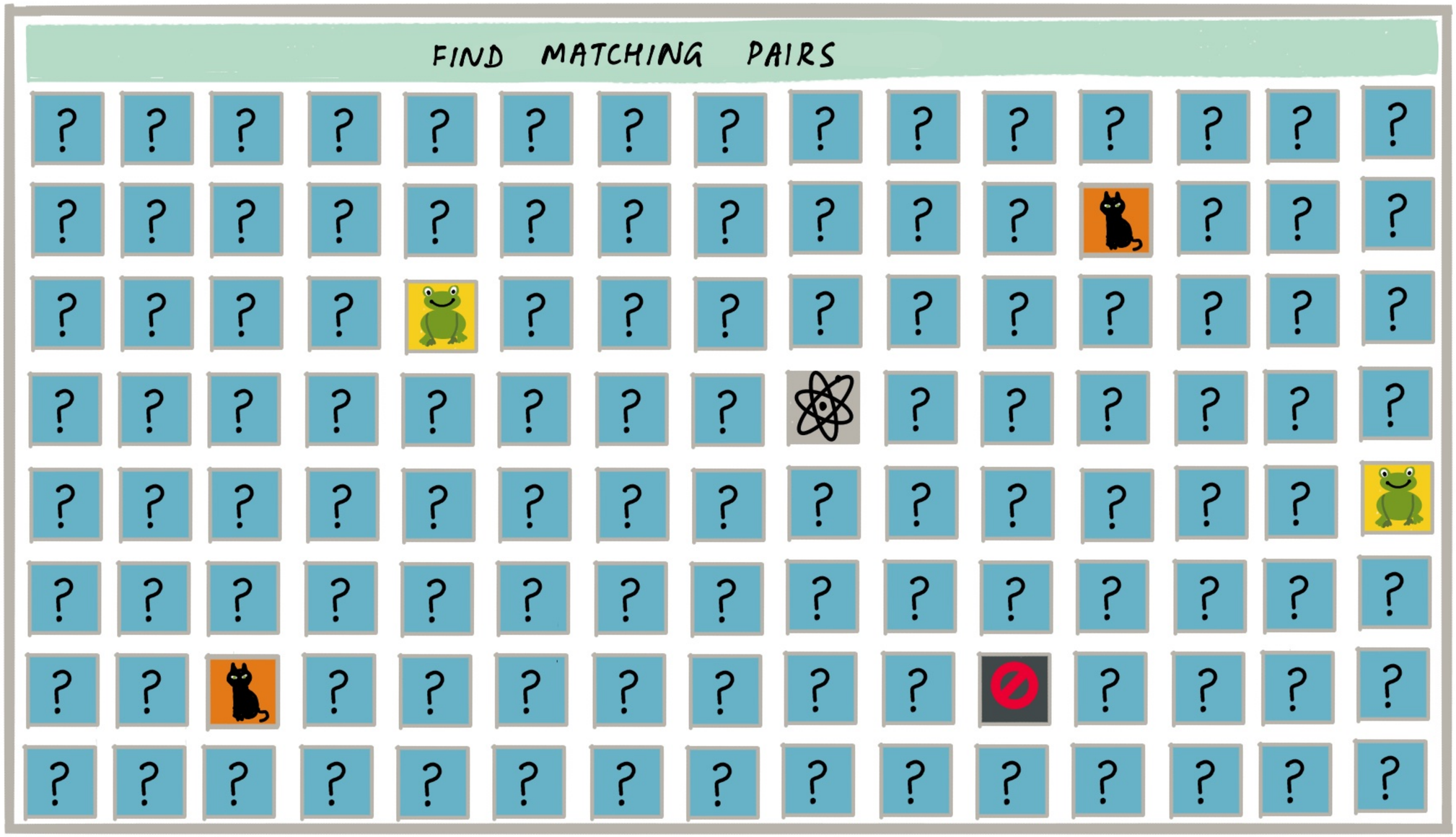
LOOK HARDER?

FIND A NEEDLE IN A HAYSTACK

FIND PRIME FACTORS OF 5893

FIND THE MATCHING PATTERN ACROSS A FEW 100 SEQUENCES

# DIFFICULTY WITH MEMORY






KEEP IN MEMORY

SHOPPING LIST OF 3 ITEMS

A 4-PIECE JIGSAW PUZZLE





HOW MUCH MORE TO RETAIN

WHEN THE LIST HAS OVER 500 ITEMS

WHEN THE PUZZLE HAS ~1000 PIECES

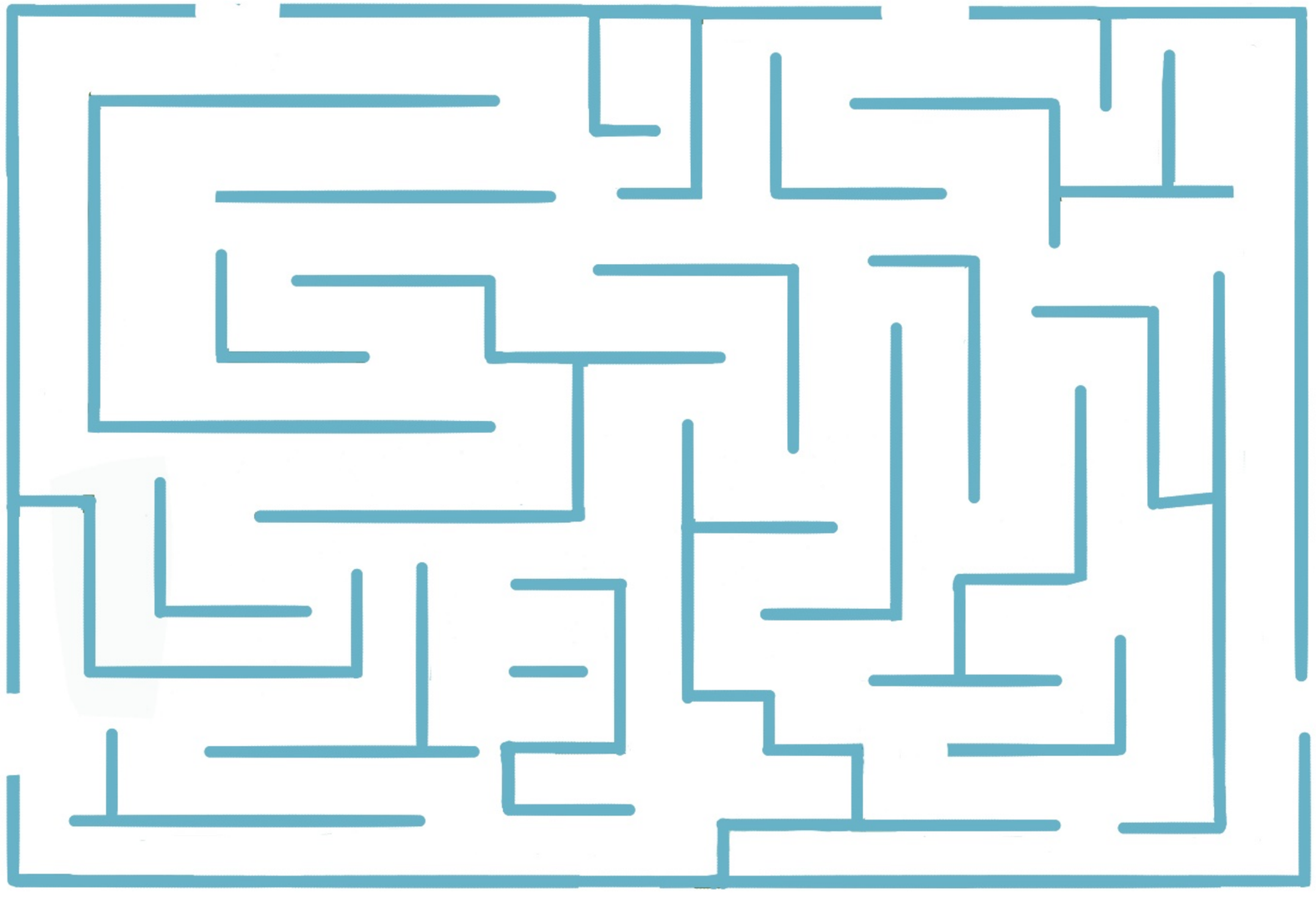
# DIFFICULTY OF OPTIONS



OPTIMISE !

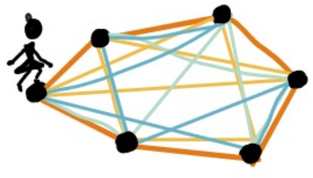


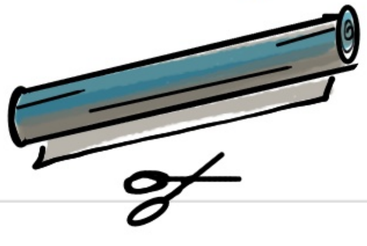






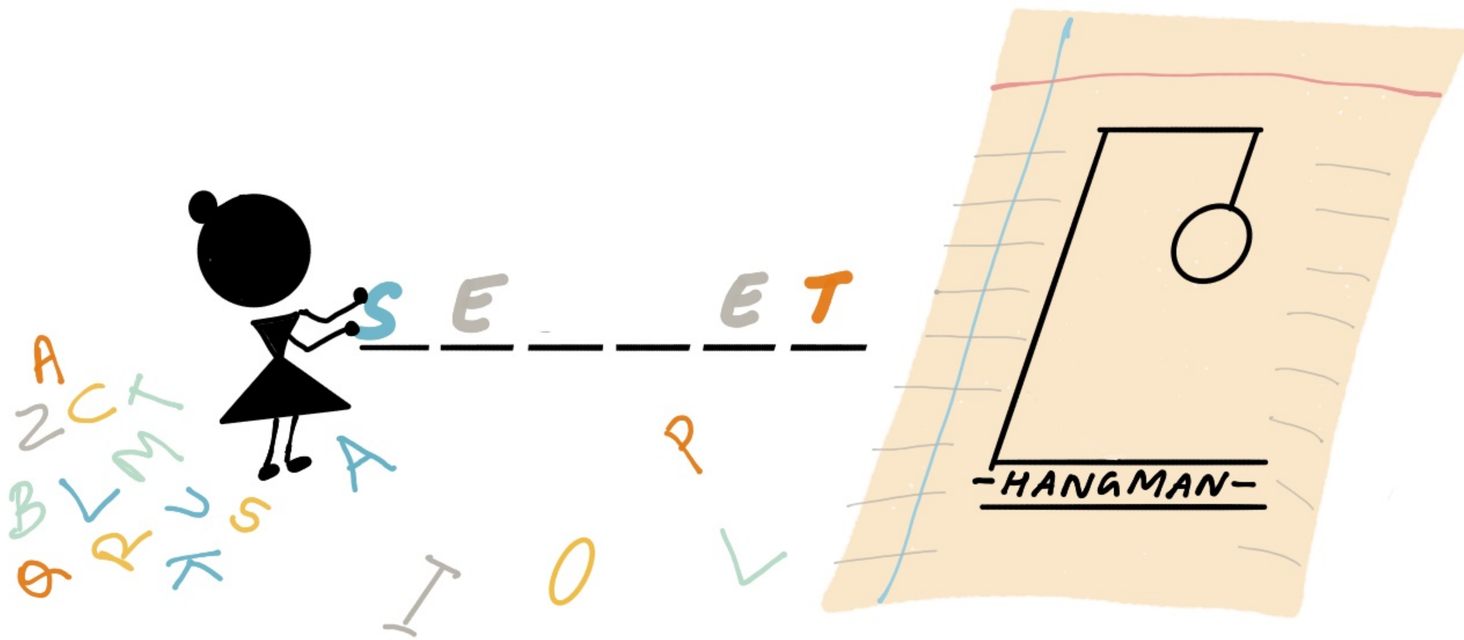

WHAT IS THE SHORTEST ROUTE ACROSS N CITIES ?





CUT A JUMBO ROLL OF PAPER INTO THE MOST NUMBER OF SIZES SUCH AS A1, A2, A3, ... WITH MINIMUM WASTE

# HOW HARD IS HANGMAN?




SOURCE : DICTIONARY

TOTAL NUMBER OF WORDS : ~ 300,000

WORD LENGTH : 6

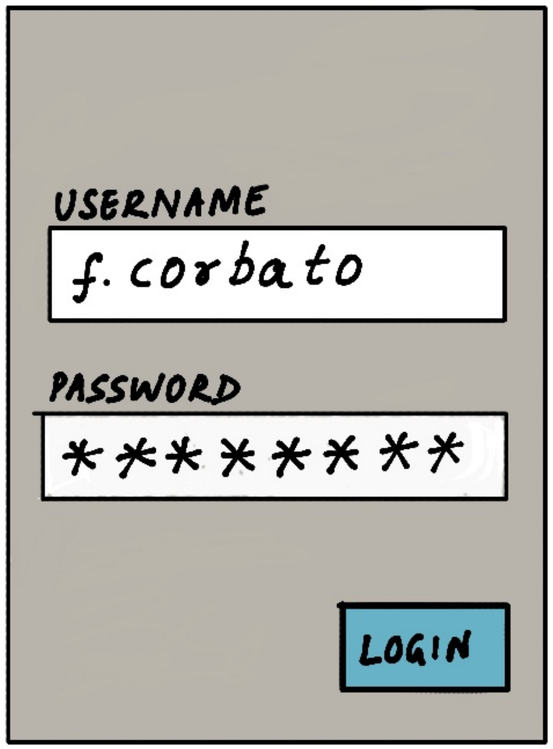
NUMBER OF 6-LETTER WORD OPTIONS: ~80,000

source : thefreedictionary.com

IT PROBABLY DOES NOT MAKE MUCH DIFFERENCE WHETHER THE WORD YOU ARE GUESSING IS 6 OR 16 LETTERS LONG

# CRACK A PASSWORD?






SOURCE : KEYBOARD

AVAILABLE KEYBOARD CHARACTERS : 85

PASSWORD LENGTH : 8

NUMBER OF 8-LETTER PASSWORD OPTIONS : ~ 2,000,000,000,000,000

calculation $= (85)^8$

A PASSWORD OF 8 LETTERS COULD BE ANY COMBINATION OF
- 0-9
- a-z A-Z
- @ # % ? * { + / - ...

THIS SET OF POSSIBILITIES IS EXPONENTIALLY LARGE —

GROWING EVEN MORE IF THE PASSWORD IS A PASSPHRASE

# HOW DOES YOUR PROBLEM GROW?

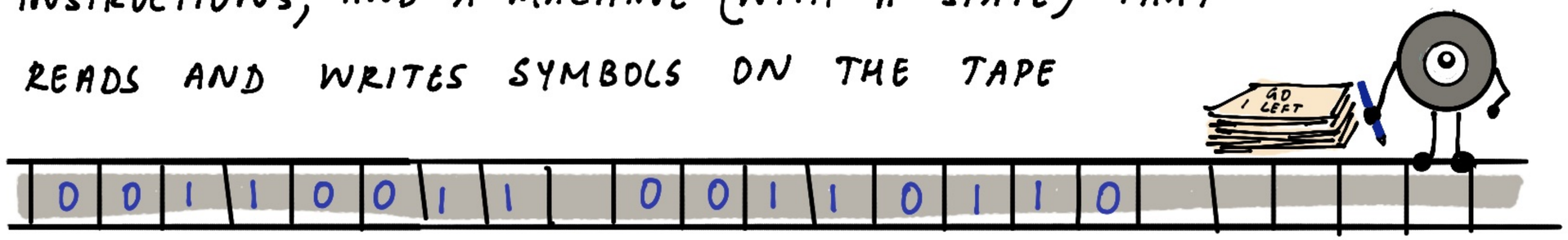
— A TOUR OF COMPUTATIONAL COMPLEXITY —

# COMPUTATIONAL COMPLEXITY



ALAN TURING
1936

ALAN TURING CAME UP WITH A MODEL OF COMPUTATION THAT WE STILL USE TODAY. IT CONSISTS OF AN INFINITELY LONG TAPE, SOME INSTRUCTIONS, AND A MACHINE (WITH A STATE) THAT READS AND WRITES SYMBOLS ON THE TAPE




ANYTHING A MODERN COMPUTER CAN DO, A TURING MACHINE CAN DO

THE VERY NOTION OF AN ALGORITHM IS BASED ON THE TURING MACHINE

AN INTERPRETATION OF THE FAMOUS CHURCH-TURING THESIS IS THAT ANYTHING COMPUTABLE CAN BE WORKED OUT BY A TURING MACHINE.

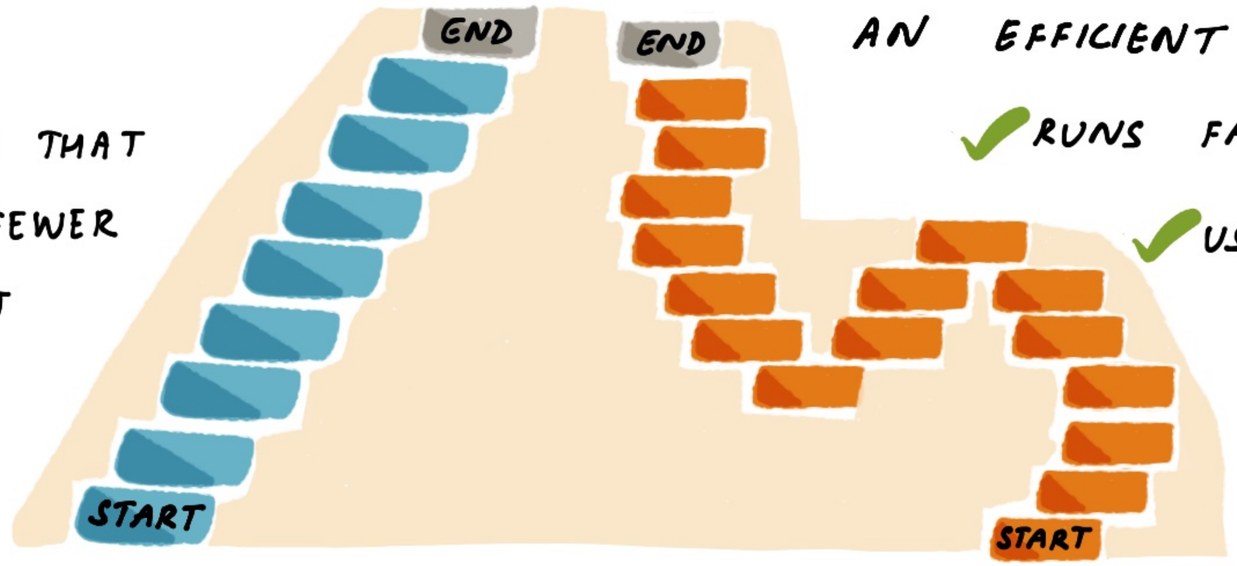
NATURALLY, THIS LED TO FURTHER INVESTIGATIONS ON WHAT THE LIMITS ARE, IF ANY, TO COMPUTATION. COMPUTATIONAL COMPLEXITY IS A FIELD THAT GREW FROM THE 1970-S.

LET US LOOK AT SOME OF THE CONCEPTS

# ALGORITHM EFFICIENCY

## WHAT IS IT?

OBVIOUSLY, AN ALGORITHM THAT ACHIEVES ITS GOAL IN FEWER STEPS IS MORE EFFICIENT

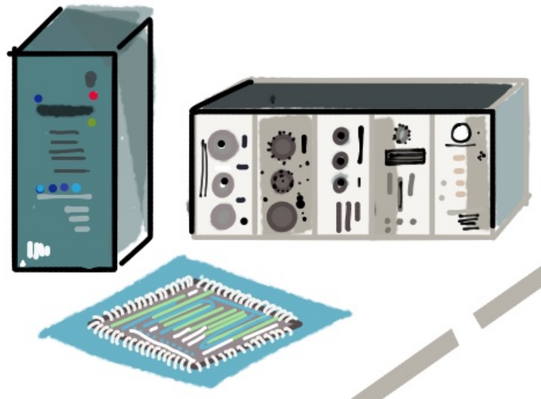



AN EFFICIENT PROGRAM

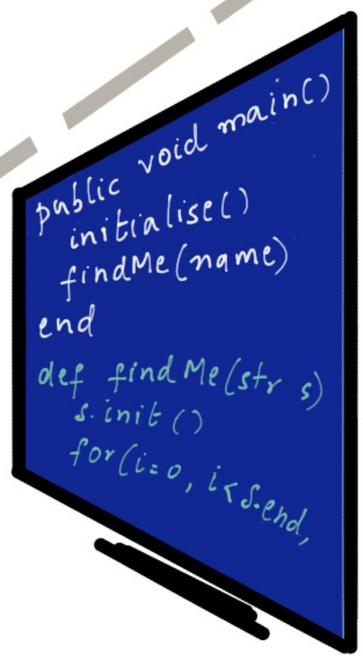
✓ RUNS FASTER

✓ USES LESS RESOURCES

## EFFICIENCY IS INDEPENDENT OF



✓ HARDWARE




✓ IMPLEMENTATION

## EFFICIENCY DEPENDS ON

INPUT SIZE

WHEN INPUT SIZE GROWS

HOW MUCH DOES RUNTIME SLOW?

THIS IS A TIME-COMPLEXITY MEASURE

# POLYNOMIAL TIME P

A PROBLEM IS IN CLASS P IF THE RUNNING TIME OF THE BEST ALGORITHM GROWS AS A POWER OF THE INPUT SIZE $n^0, n^1, n^2, n^3, n^4, \ldots$

**CLASS P PROBLEMS ARE SOLVED IN ACHIEVABLE/REASONABLE TIME**

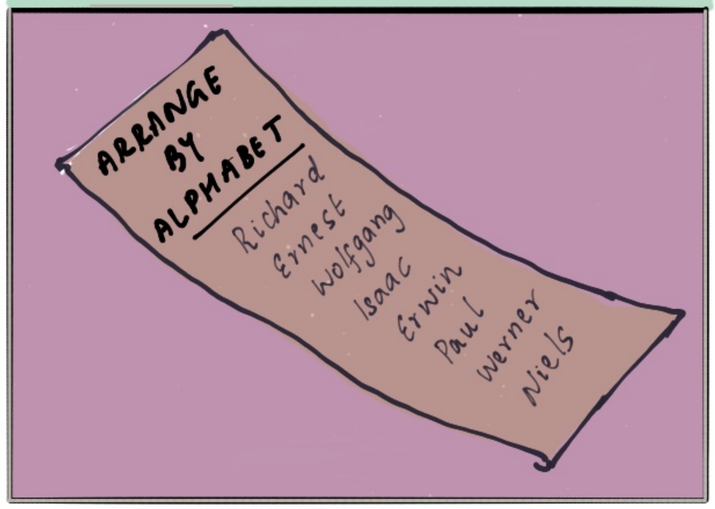
JOBS THAT A DESKTOP/SMARTPHONE CAN DO ARE IN P
SUCH AS FINDING ROUTES, SEARCHING, PLAYING GAMES

EXAMPLES

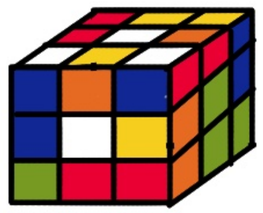
## MULTIPLY

$$\begin{array}{r} 22 \times \\ 22 \\ \hline 44 \\ 44 \\ \hline 484 \end{array} \qquad \begin{array}{r} {\scriptstyle 2} \\ 35 \times \\ 15 \\ \hline 155 \\ 35 \\ \hline 505 \end{array}$$

## SORT




## SOLVE RUBIK'S CUBE



# NON DETERMINISTIC POLYNOMIAL TIME : NP

SOME PROBLEMS APPEAR MUCH HARDER THAN P, TAKING FAR LONGER TO SOLVE

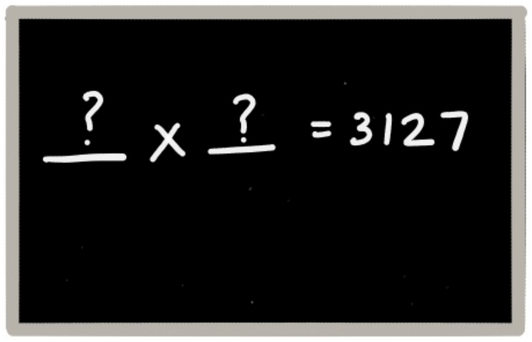
A PROBLEM IS IN CLASS NP WHEN ITS SOLUTION CAN BE EASILY CHECKED

CLASS NP PROBLEMS ARE VERIFIABLE IN POLYNOMIAL TIME

MANY OF THE NP PROBLEMS CAN BE THOUGHT OF AS SEARCHING THROUGH A LOT OF POSSIBILITIES

EXAMPLES

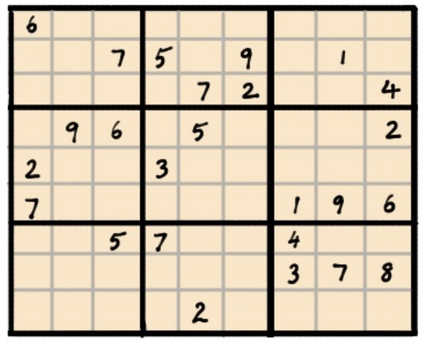
### FACTORISE A NUMBER




### PACK A SUITCASE



### SOLVE A SUDOKU




FACTORISATION IS A CORE STEP IN ENCRYPTION INVOLVING RSA

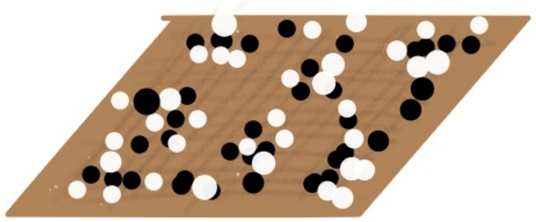
# NOT POLYNOMIAL TIME

UNSURPRISINGLY, THERE ARE ALSO PROBLEMS THAT CAN NEITHER BE SOLVED NOR VERIFIED IN POLYNOMIAL TIME

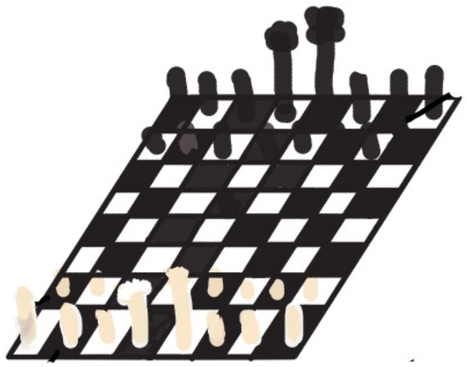
FOR SOME PROBLEMS, THERE IS PROOF THAT THEY CANNOT BE SOLVED AND FOR SOME, THERE ISN'T EVEN A PROOF

## EXAMPLES

GO



CHESS



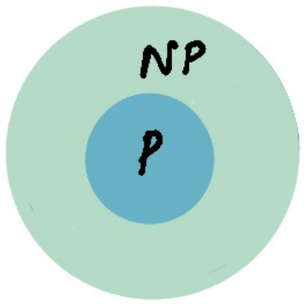
There is a far more detailed hierarchy of difficulty levels - based on formal definitions and evolving from new research

EXERCISE : LOOKUP - complexity200.uwaterloo.ca

# P vs NP

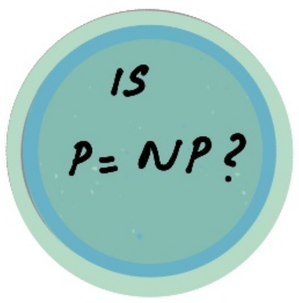
P — EFFICIENTLY SOLVED PROBLEMS

NP — EFFICIENTLY VERIFIED PROBLEMS




NP CONTAINS P

THE ALGORITHM FOR SOLVING THE PROBLEM, BY BEING CORRECT, VERIFIES THE SOLUTION




IS P=NP ?

CAN EFFICIENTLY VERIFIED PROBLEMS BE EFFICIENTLY SOLVED TOO ?

IT IS BELIEVED THAT $P \neq NP$

BUT THERE IS NO PROOF

THIS IS A MAJOR UNSOLVED PROBLEM IN COMPUTER SCIENCE / MATHEMATICS. SO IMPORTANT THAT CLAYMATH.ORG OFFERS $1M FOR THE ANSWER

✓ IF P=NP

IT GREATLY INCREASES THE SCOPE OF WHAT WE CAN KNOW AND DISCOVER (and most crypto would break)

✗ IF $P \neq NP$

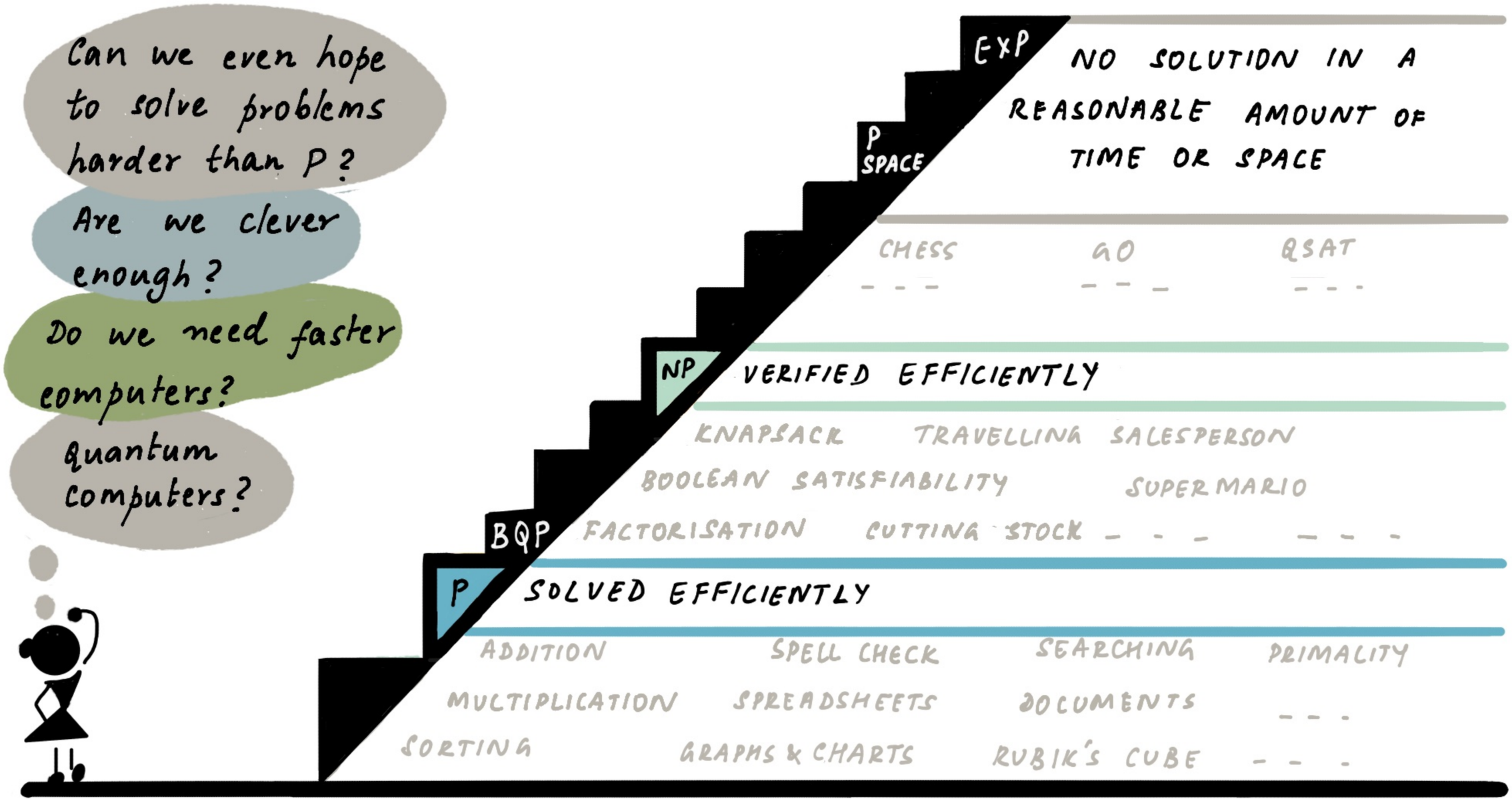
ARE WE LEFT WITH ALGORITHMS THAT GO THROUGH EVERY OPTION UNTIL ... THE END OF THE WORLD...

ARE WE TO ACCEPT THAT THERE ARE PROBLEMS WE CANNOT SOLVE...

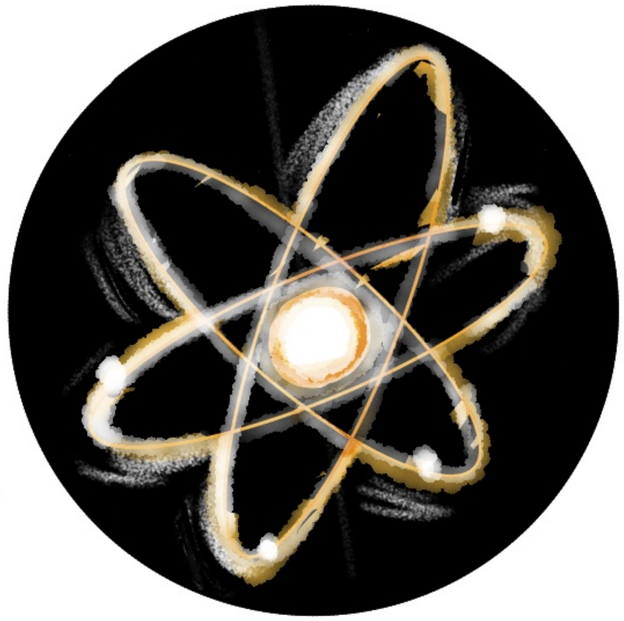
LIKE GÖDEL SHOWED THAT THERE ARE TRUE ARITHMETIC STATEMENTS THAT AXIOMS IN MATHS CAN'T HELP TO PROVE

LIKE TURING SHOWED THAT THERE IS NO PROGRAM THAT CAN DECIDE IF ANOTHER PROGRAM WILL HALT OR NOT...

# WHAT OPTIONS DO WE HAVE?



# SO, QUANTUM...



QUANTUS IS LATIN FOR 'HOW GREAT'

QUANTUM IS THE SMALLEST 'PIECE' OF ENERGY

QUANTUM MECHANICS DESCRIBES NATURE AT THE TINIEST OF SCALES

THE NOTION OF QUANTUM CAME AT A TIME WHEN THE PHENOMENA IN THE MACRO/CLASSICAL WORLD HAD BEEN WELL EXPLAINED BY MATHEMATICAL FORMULAE

# THE CLASSICAL WORLD VIEW



NEWTON LAID OUT A DETERMINISTIC PICTURE OF OUR WORLD

HIS MATHEMATICS DESCRIBED AND PREDICTED —



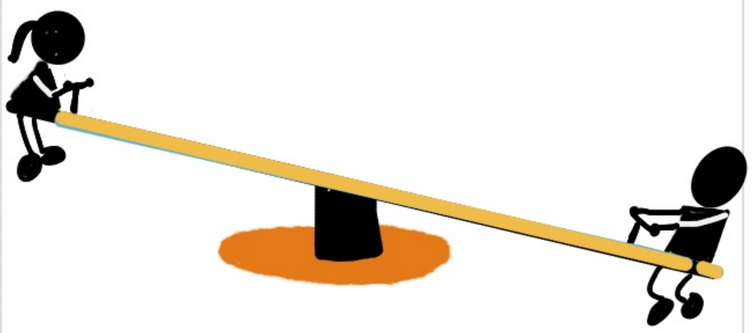
ACCELERATION

INERTIA



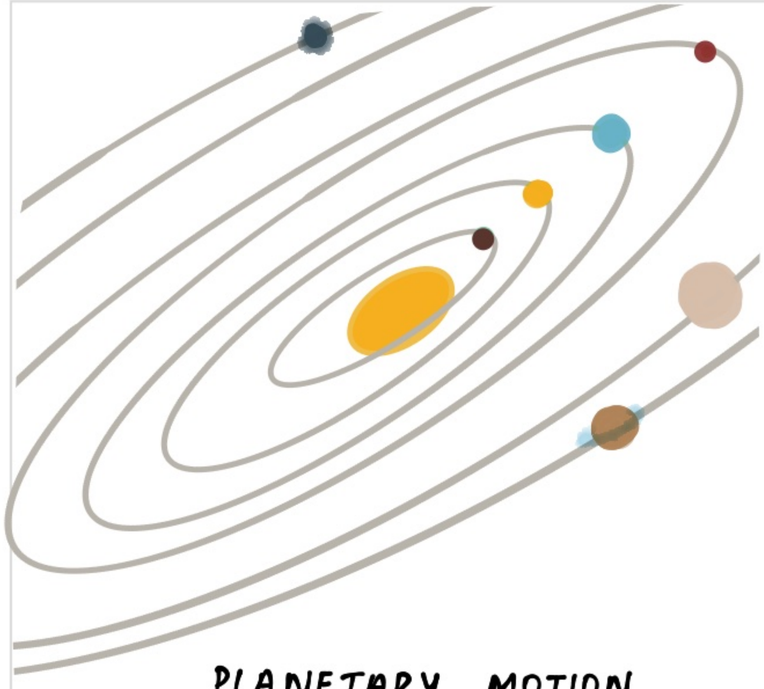
VELOCITY

MOMENTUM



ACTION

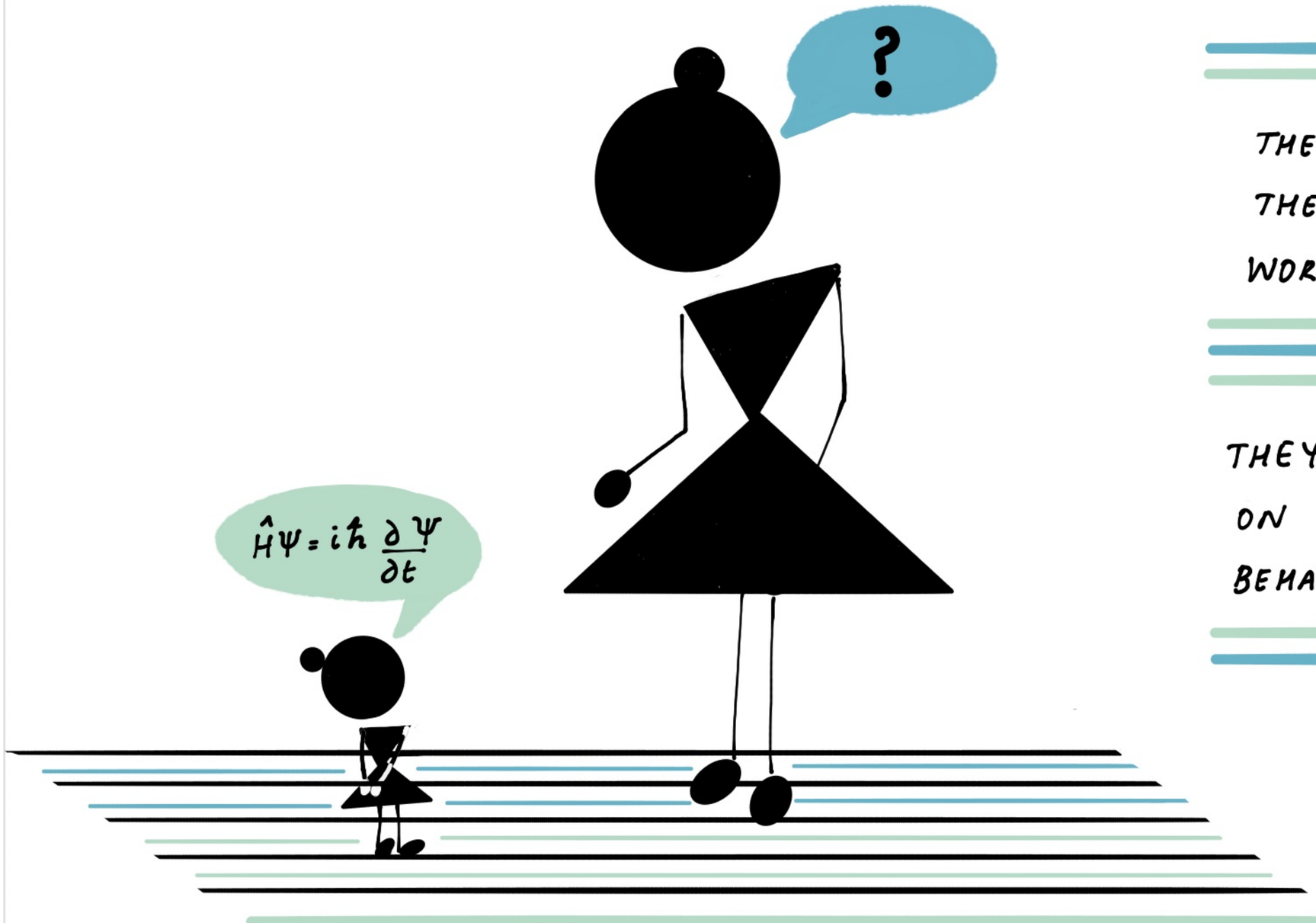
REACTION



PLANETARY MOTION

THIS PREDICTABLE CLOCKWORK VIEW OF THE UNIVERSE WAS SOON GOING TO CHANGE

# QUANTUM Vs CLASSICAL




THE QUANTUM AND THE CLASSICAL ARE WORLDS APART

THEY SEEM TO OPERATE ON DIFFERENT LAWS BEHAVE DIFFERENTLY

HOW DO WE BEGIN TO UNDERSTAND OR COMPARE THE TWO?

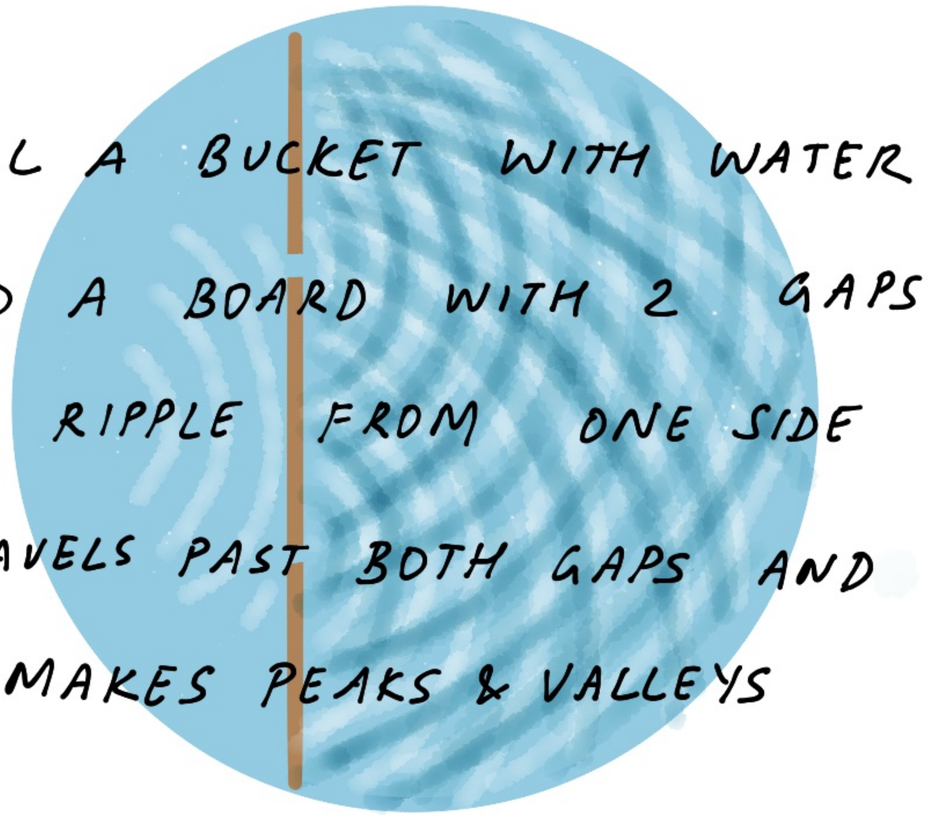
A GOOD PLACE TO START IS TO LOOK AT PARTICLES & WAVES

# A SIMPLE EXPERIMENT

TO REMIND US

WHAT PARTICLES DO

WHAT WAVES DO



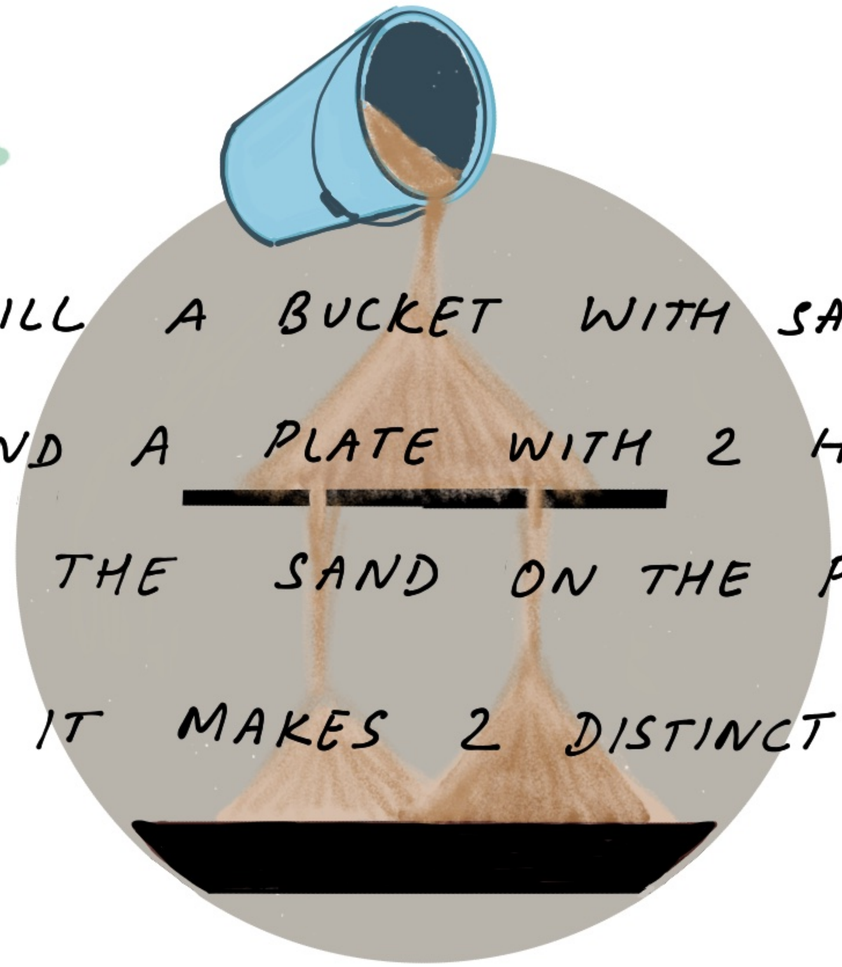
FILL A BUCKET WITH WATER

FIND A BOARD WITH 2 GAPS

A RIPPLE FROM ONE SIDE

TRAVELS PAST BOTH GAPS AND

MAKES PEAKS & VALLEYS



FILL A BUCKET WITH SAND

FIND A PLATE WITH 2 HOLES

POUR THE SAND ON THE PLATE

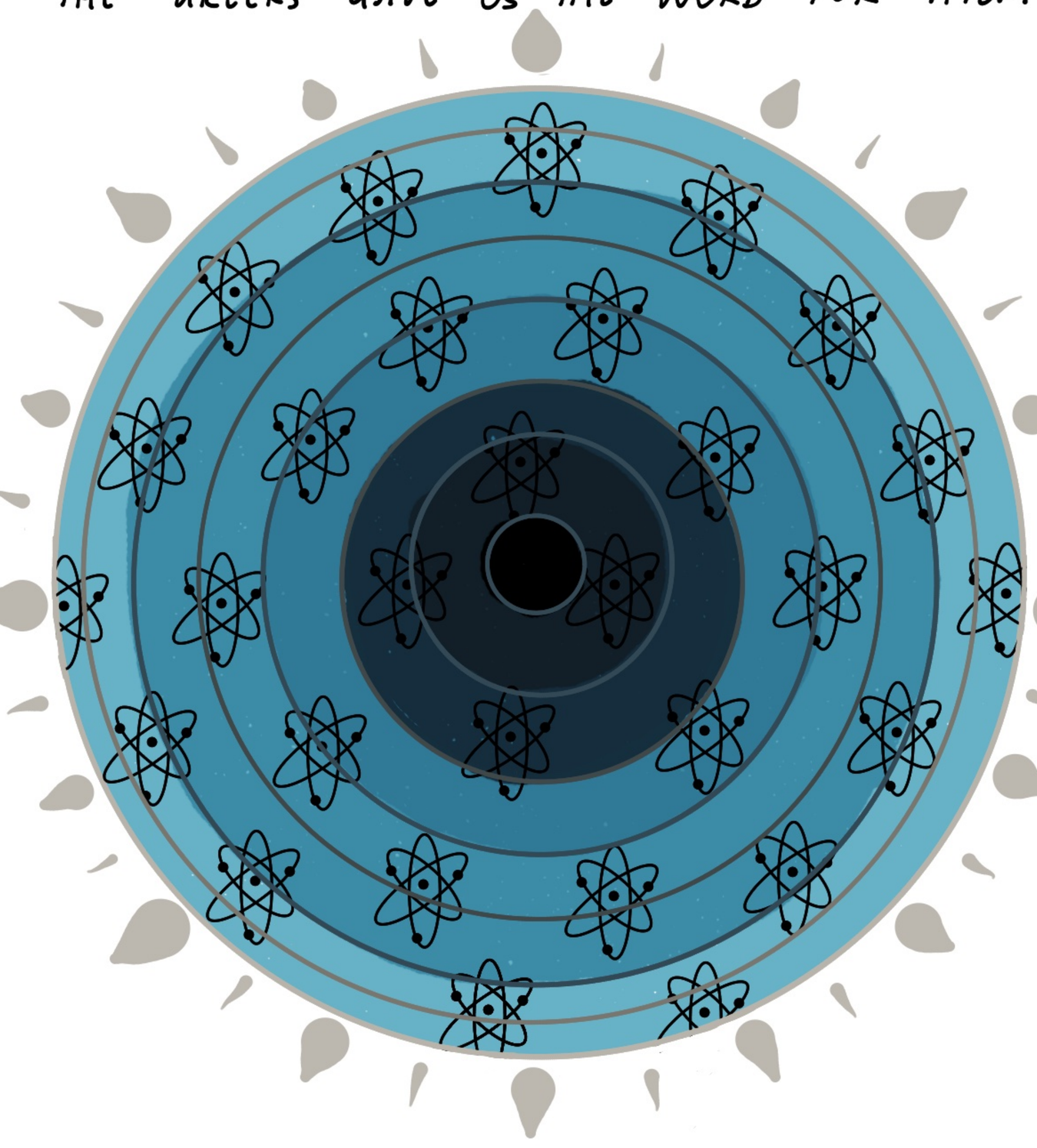
SEE IT MAKES 2 DISTINCT PILES

WHY IS THIS RELEVANT?

BECAUSE SIMILAR EXPERIMENTS IN THE QUANTUM WORLD GAVE VERY UNEXPECTED RESULTS.

# THE SUBATOMIC WORLD

THE GREEKS GAVE US THE WORD FOR ATOM



BUT IT TOOK THE MIND OF ALBERT EINSTEIN TO PROVE THAT ATOMS EXIST

THIS WAS PROBABLY OUR FIRST PEEK INTO THE QUANTUM WORLD

THE FASCINATION WITH LIGHT HOWEVER, BROUGHT US CLOSER TO UNDERSTANDING 'QUANTUMNESS'

# AT FIRST IT WAS LIGHT

WHAT IS LIGHT?

ANCIENT GREEKS THOUGHT THAT A BEAM FROM THE EYES ENABLED US TO SEE

IS LIGHT WHITE?
WHAT DOES IT WEIGH?
IS IT INFINITELY FAST?

LIGHT BOUNCES, SCATTERS, BENDS, DIFFRACTS, ...
WHY?

THE PURSUIT OF THESE QUESTIONS AND THE DESIRE TO USE AND CONTROL LIGHT LED TO INTERESTING ANSWERS AND DISCOVERIES

LIGHT IS MADE OF CORPUSCLES



ISAAC NEWTON

1690s

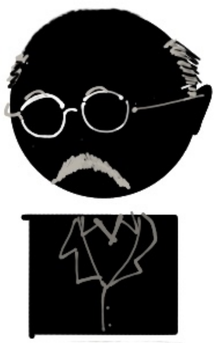
LIGHT IS REALLY WAVES



CHRISTIAAN HUYGENS

1690s

ENERGY EXISTS AS PACKETS



MAX PLANCK

1900

LIGHT TRAVELS AS PACKETS - PHOTONS



ALBERT EINSTEIN

1905

# THE BEGINNING OF QUANTUM THEORY

THUS BEGAN A RICH FIELD OF STUDY—

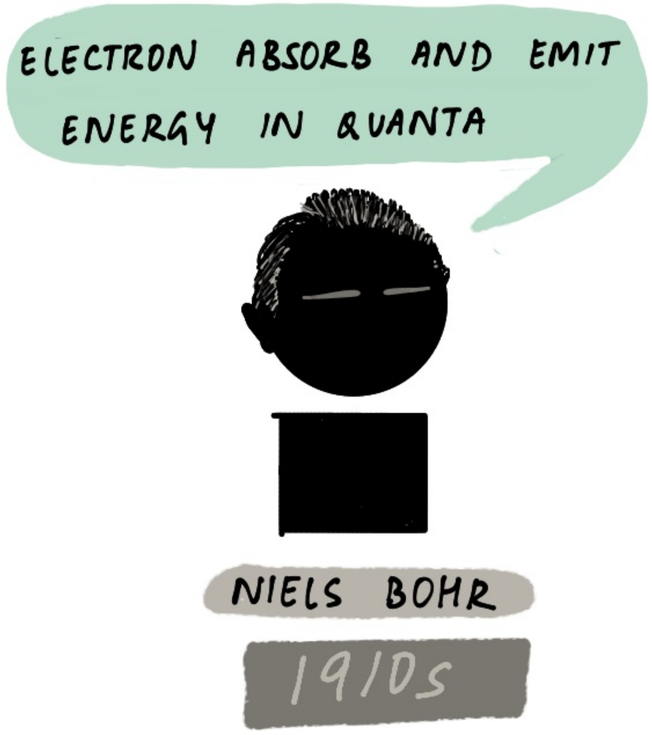
WITH CONTRIBUTIONS FROM SCIENTISTS LIKE

- PAUL DIRAC
- WOLFGANG PAULI
- MAX BORN

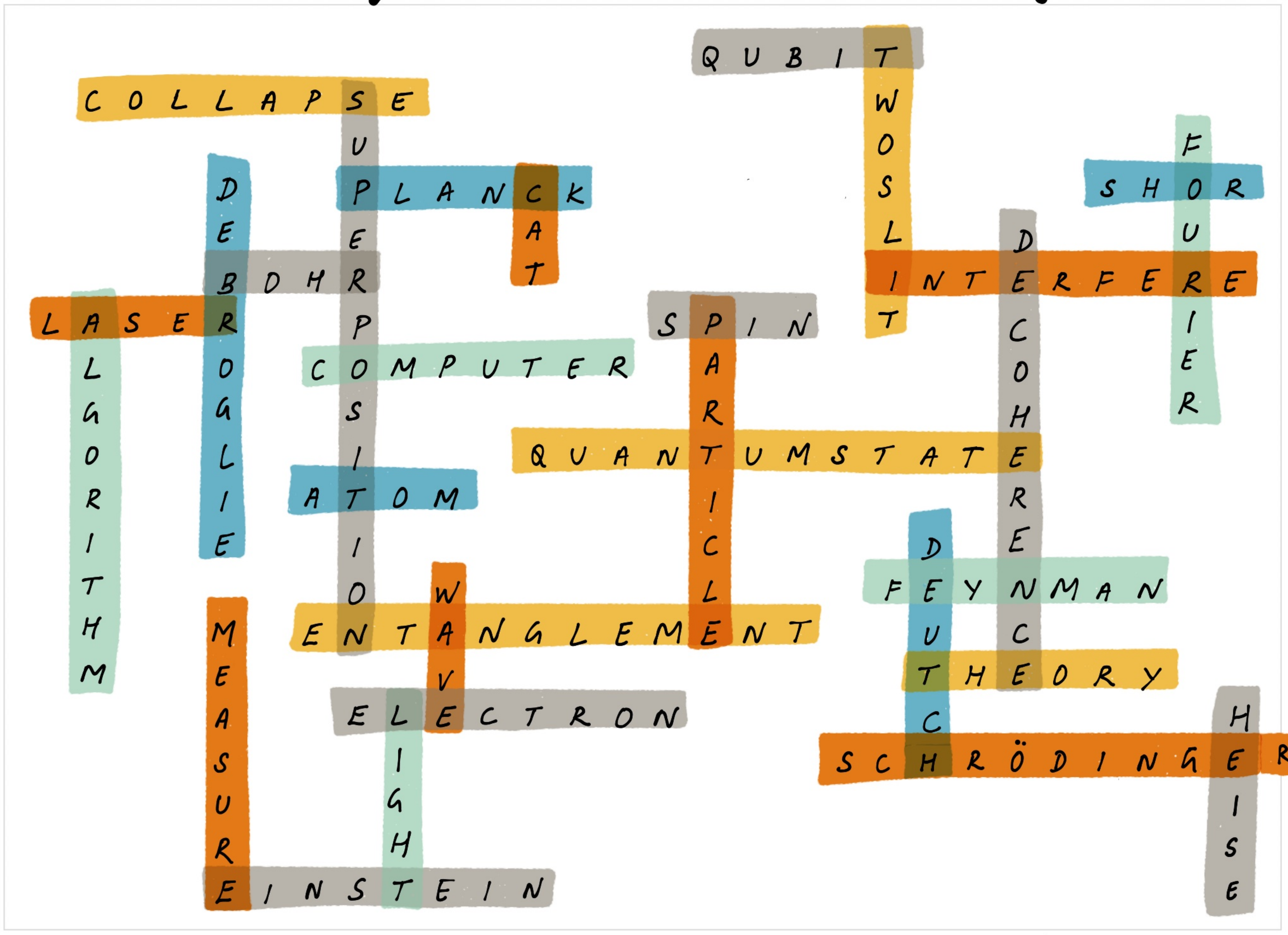
THIS FIELD IS NOW CALLED QUANTUM MECHANICS—
AND IT SEEMS TO ESTABLISH:

WE CANNOT KNOW EVERYTHING ABOUT NATURE'S BUILDING BLOCKS

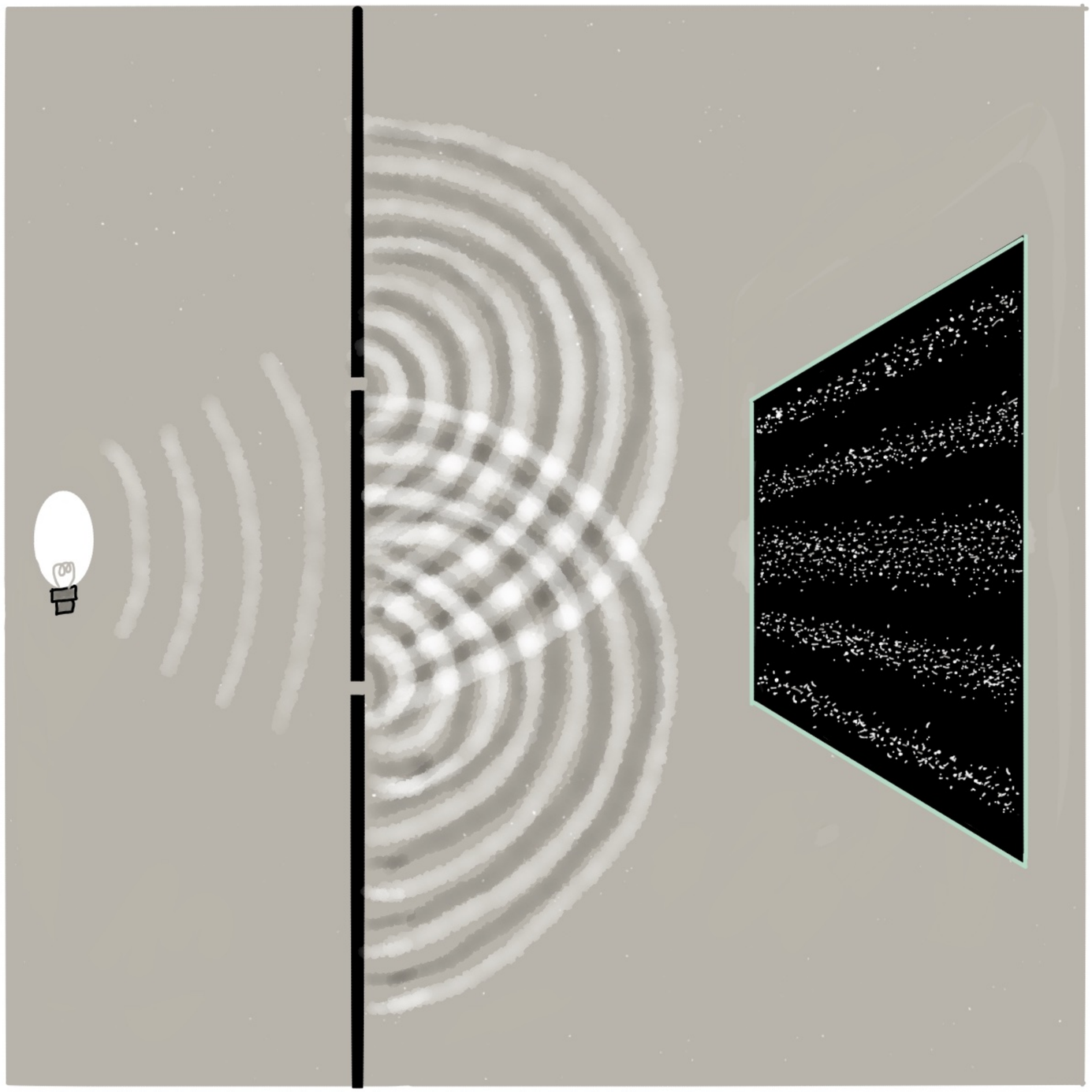
AT THE SMALLEST SCALE NATURE IS UNPREDICTABLE



# OBVIOUSLY, A NEW VOCABULARY



# BUT FIRST, THE EXPERIMENT: WITH LIGHT



EXPERIMENT BY THOMAS YOUNG 1800s

LIGHT (PHOTONS)

SHONE THROUGH

TWO NARROW SLITS

FORM ALTERNATE

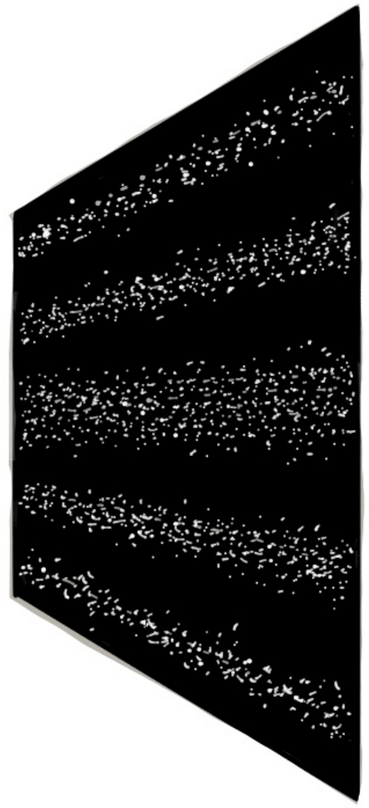
DARK AND LIGHT BANDS

AN INTERFERENCE PATTERN

# PHOTON PEEKABOO

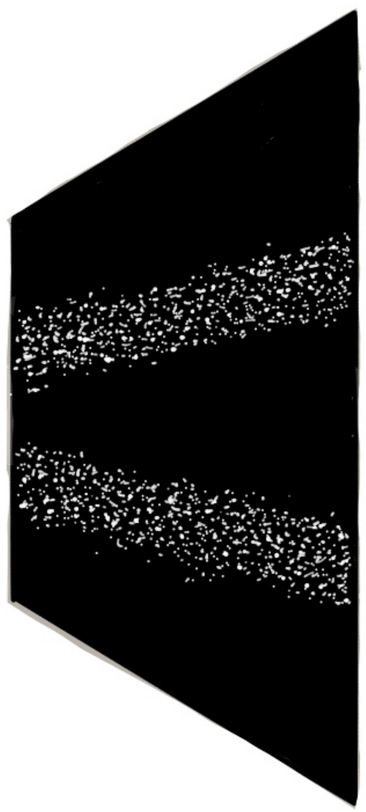
IT SEEMS,
WHEN LEFT ALONE
PHOTONS PASS THROUGH
BOTH SLITS

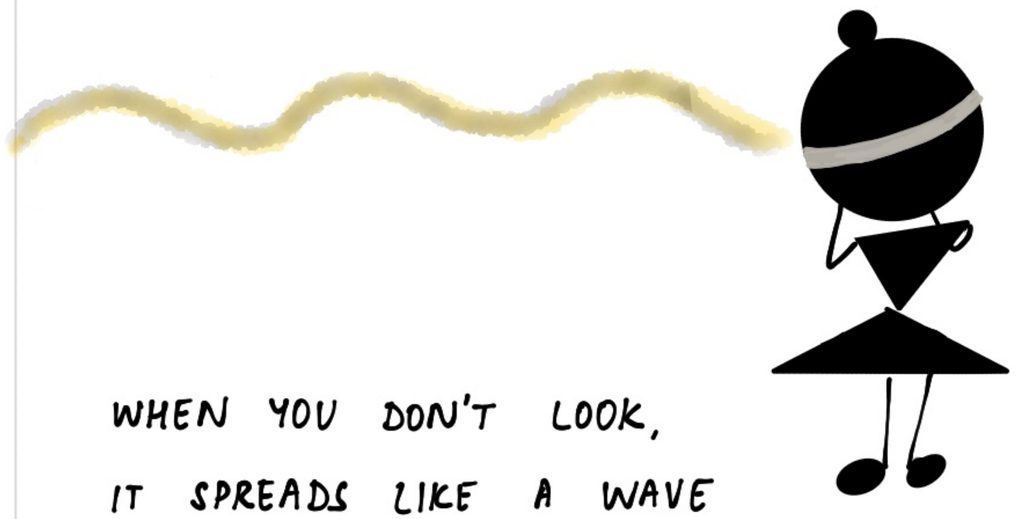
LIKE A RIPPLE
THROUGH WATER



ADD A DETECTOR
TO SEE WHICH SLIT
THE PHOTONS USED

THEN,
LIKE POURING SAND
TWO BANDS FORM





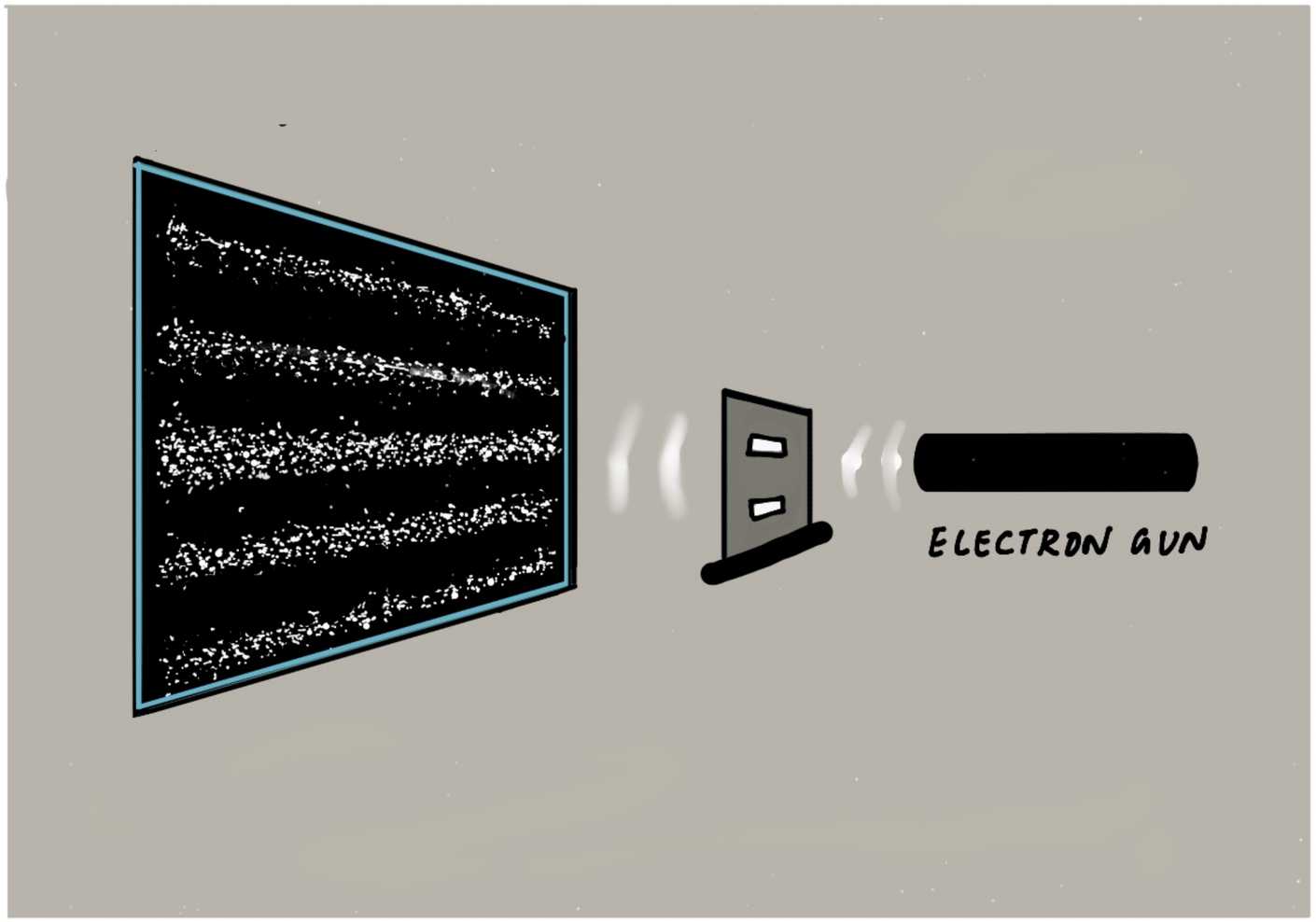
WHEN YOU DON'T LOOK,
IT SPREADS LIKE A WAVE



WHEN YOU LOOK
IT 'COLLAPSES' TO A PARTICLE

# THE EXPERIMENT: WITH MATTER

CURIOUSLY, ELECTRONS SENT ONE BY ONE ALSO FORM THE INTERFERENCE PATTERN.




EXPERIMENT BY DAVISSON/THOMSON 1920s

THE STUFF THAT MATTER IS MADE OF BEHAVES LIKE WAVES

"THERE ARE SITUATIONS WHEN A PARTICLE MAY NOT HAVE A LOCATION AT ALL"

- BRIAN GREENE

HOW DOES THIS RECONCILE WITH NEWTON'S VERY PREDICTABLE PHYSICS?

AN OUTCOME (NEARLY) IMPOSSIBLE TO UNDERSTAND OR EXPLAIN

# QUANTUM WEIRDNESS

THE UNFAMILIAR, WEIRD BEHAVIOUR COMMON TO ALL THINGS QUANTUM IS FILED UNDER:

- SUPERPOSITION
- ENTANGLEMENT

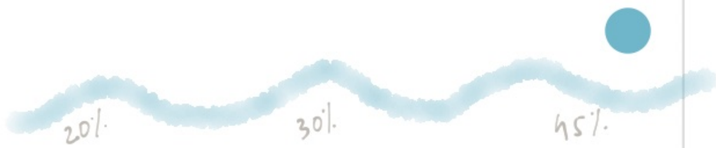
LET US FIRST LOOK AT THEM CONCEPTUALLY FROM A CLASSICAL VIEW

THEN POKE INTO THEIR NATURE MORE CLOSELY. WITH A MATHEMATICAL LENS.

# QUANTUM SUPERPOSITION

THE QUANTUM PARTICLE
(e.g. PHOTON, ELECTRON)
SPREADS OUT LIKE A WAVE

IT "EXISTS" AS A
WAVE OF PROBABILITY




A STATE OF BEING IN
MULTIPLE LOCATIONS AT ONCE
EACH WITH A DIFFERENT PROBABILITY




JUST AS WAVES IN WATER ADD UP
TO FORM A RESULTANT WAVE...



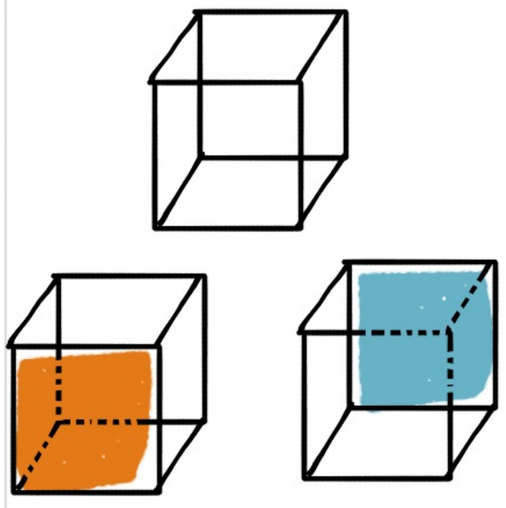


...QUANTUM STATES ADD UP TO FORM
A SUPERPOSITION

# SUPERPOSITION: A MACRO PICTURE



HARD TO EXPRESS IN THE CLASSICAL WORLD



A COIN BEING FLIPPED

IS HEADS

IS TAILS

A MIX OF BOTH

WITH A 50-50 CHANCE

THE SCIENTIST'S CAT

NEXT TO SOME POISON

IS ALIVE

IS DEAD

A CUBE YOU SEE

WHAT FACE IS IN FRONT?

THE BLUE?

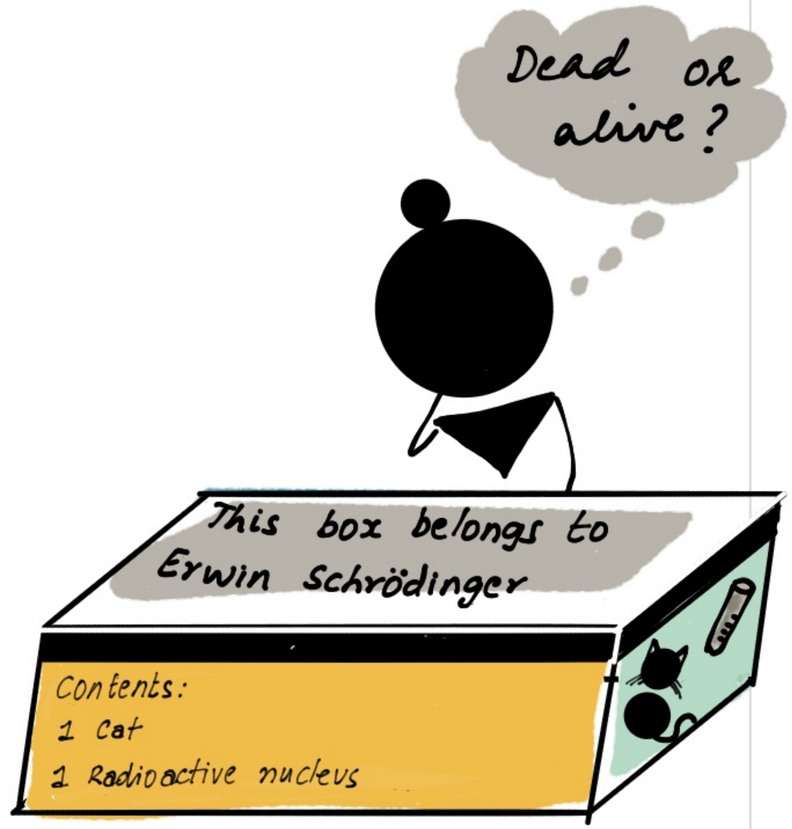
THE ORANGE?

AN ELECTRON WITH SPIN

THAT'S UP

THAT'S DOWN

UNTIL YOU CHECK!






# EINSTEIN WASN'T A FAN

WE CANNOT KNOW WHERE AN ELECTRON IS - UNTIL WE MEASURE IT



NIELS BOHR

WHY DO WE NEVER SEE A HALF-ALIVE-HALF-DEAD CAT FOR REAL?

IF I AM MADE OF ELECTRONS THEN, AM I TOO SPREADING OUT - LIKE A WAVE?

THE MOON DOES NOT CEASE TO EXIST WHEN YOU STOP LOOKING AT IT



ALBERT EINSTEIN

EINSTEIN WROTE A PAPER TO SAY THAT QUANTUM MECHANICS WASN'T COMPLETE. AND THAT IT COULD NOT EXPLAIN ITS OWN PREDICTION OF ENTANGLEMENT.

# ENTANGLEMENT: THE CORRELATION



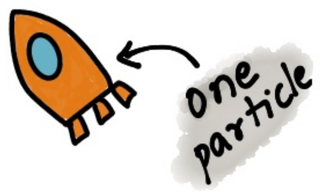
UNDER THE RIGHT CONDITIONS
TWO ELECTRONS
OR PHOTONS
CAN BE ENTANGLED

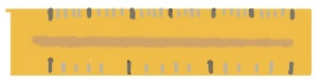


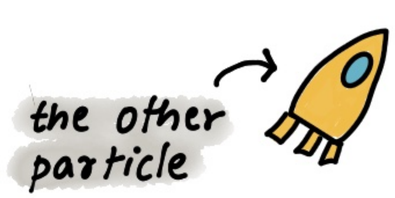
THIS MEANS:
THE PROPERTIES OF THE TWO PARTICLES
ARE "RELATED" EVEN IF THE
PARTICLES ARE SEPARATED










MEASURING ONE
INSTANTLY DECIDES THE
STATE OF THE OTHER
FASTER THAN THE SPEED OF LIGHT!

[ENTANGLED COINS WOULD
BOTH MEASURE HEADS]

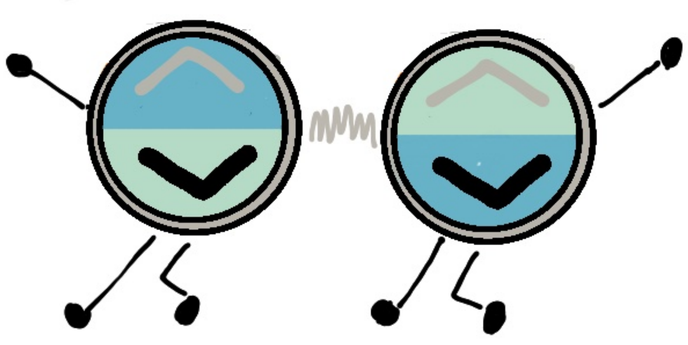




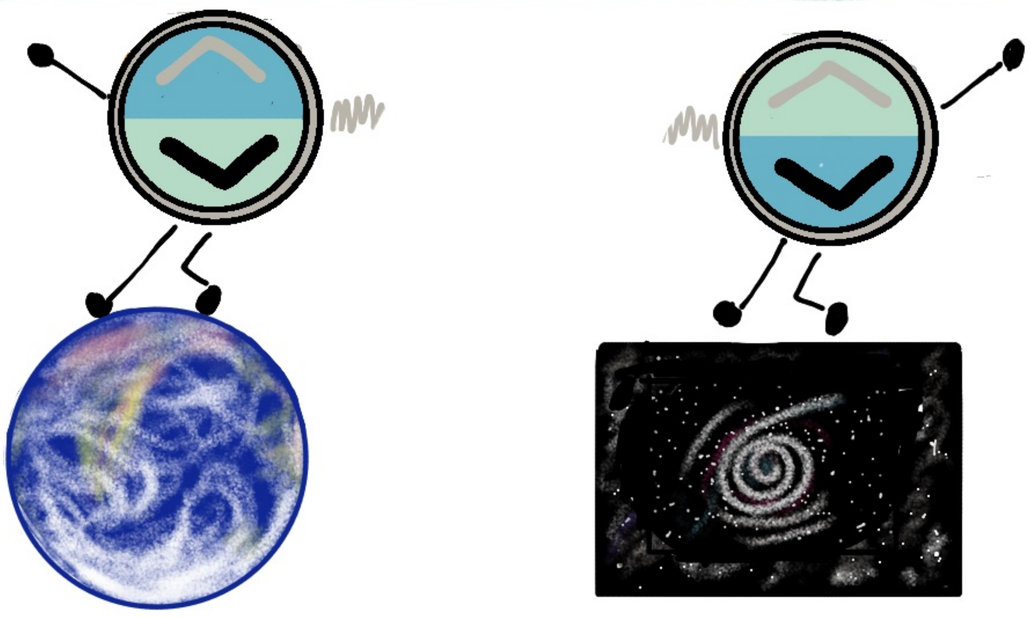

# ENTANGLED PARTICLES

INFLUENCE EACH OTHER'S STATE EVEN IF THEY ARE GALAXIES APART

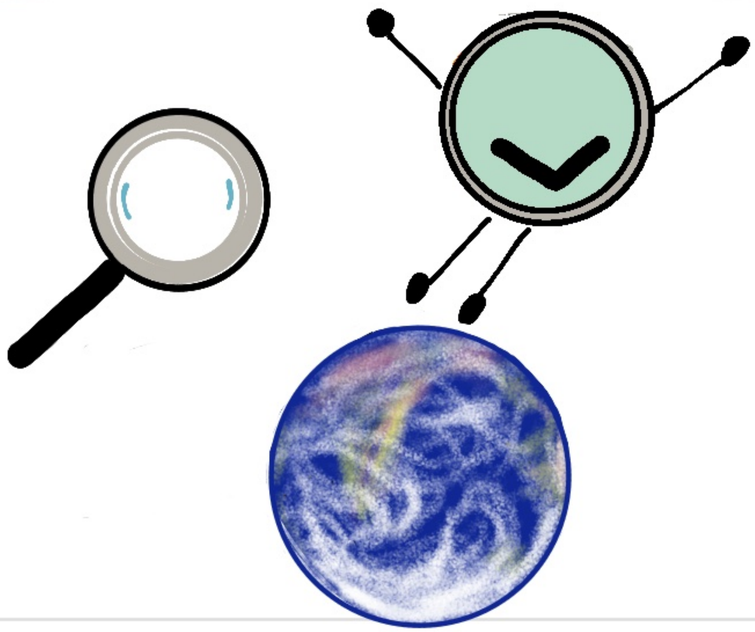
## ENTANGLE



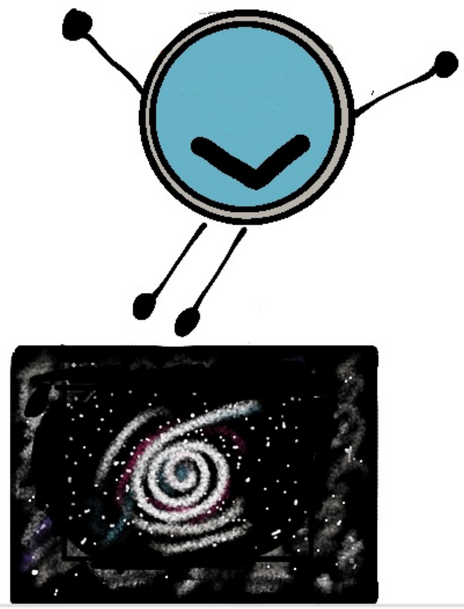
## SEPARATE



## MEASURE ONE

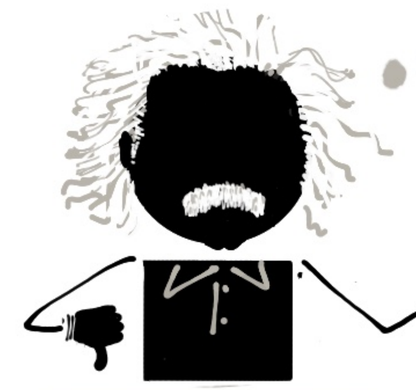


## THE OTHER WILL MATCH



# ENTANGLEMENT CONUNDRUMS

Entanglement? It is spooky action at a distance!



ALBERT EINSTEIN

CAN QUANTUM MECHANICAL DESCRIPTION OF PHYSICAL REALITY BE COMPLETE?
- EINSTEIN
- PODOLSKY
- ROSEN

1935

faster than Light? Never!

any correlation would have to be predetermined

EINSTEIN'S FINAL PAPER ARGUES THAT ENTANGLEMENT HAS A PREDETERMINED OUTCOME

NOTHING CAN TRAVEL FASTER THAN THE SPEED OF LIGHT

IF ENTANGLED PARTICLES ACROSS GALAXIES COULD 'TALK' AND INFLUENCE EACH OTHER'S STATE THE MESSAGES WOULD TRAVEL

SHOCKING, BECAUSE IT WOULD TAKE LIGHT YEARS TO TRAVEL BETWEEN GALAXIES

# REACTIONS TO QUANTUM MECHANICS

IF QUANTUM MECHANICS HASN'T PROFOUNDLY SHOCKED YOU, YOU HAVEN'T UNDERSTOOD IT

– NIELS BOHR

I THINK I CAN SAFELY SAY THAT NO ONE UNDERSTANDS QUANTUM MECHANICS

– RICHARD FEYNMAN

I DON'T LIKE IT AND I'M SORRY I HAD ANYTHING EVER TO DO WITH IT

–ERWIN SCHRÖDINGER

GOD DOES NOT PLAY DICE

–ALBERT EINSTEIN

QUANTUM MECHANICS IS THE OPERATING SYSTEM THAT OTHER PHYSICAL THEORIES RUN ON AS APPLICATION SOFTWARE

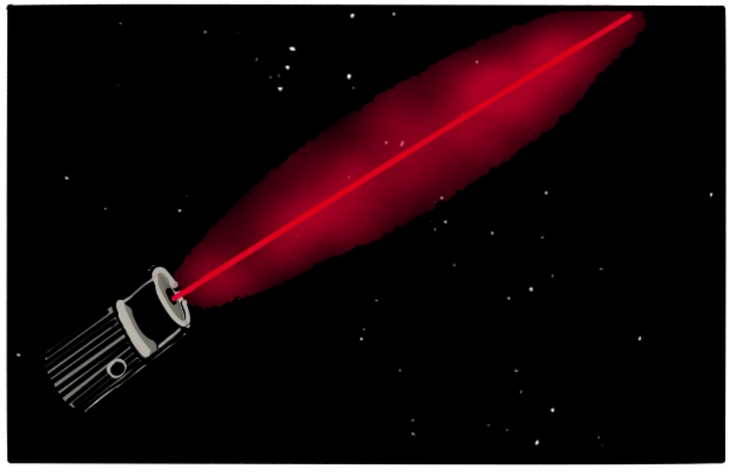


SCOTT AARONSON

# WHAT GOOD IS QUANTUM MECHANICS?

QUANTUM MECHANICS IS RESPONSIBLE FOR DEVELOPING

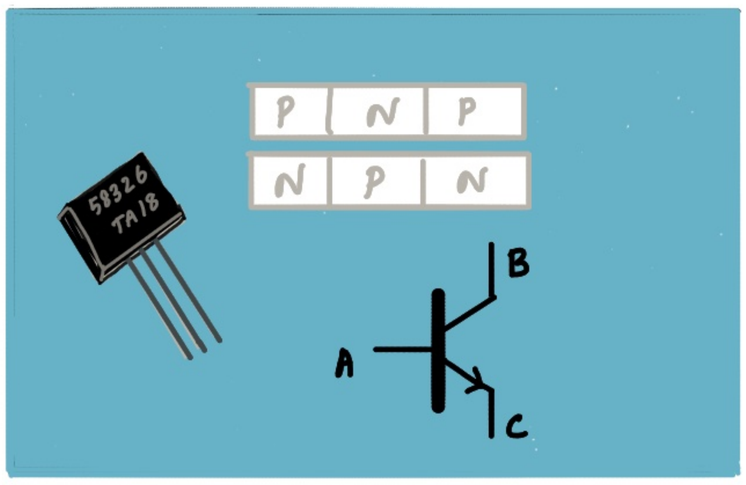
## LASERS



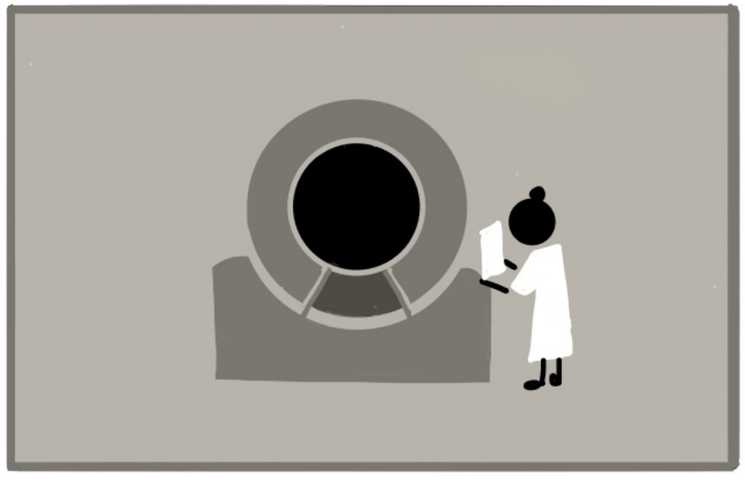
## NUCLEAR REACTIONS



## TRANSISTORS




## MEDICAL DEVICES



# QUANTUM IN COMPUTERS ?

THE IDEA OF A QUANTUM COMPUTER CAME FROM



RICHARD FEYNMAN

IF YOU WANT A SIMULATION OF NATURE, YOU'D BETTER MAKE IT QUANTUM MECHANICAL

1981

Simulating Physics with computers

by

RICHARD FEYNMAN

AND HOW IT MIGHT WORK WAS SUGGESTED BY



DAVID DEUTSCH

EVERY FINITELY REALISABLE PHYSICAL SYSTEM CAN BE PERFECTLY SIMULATED BY A UNIVERSAL MODEL COMPUTING MACHINE OPERATING BY FINITE MEANS

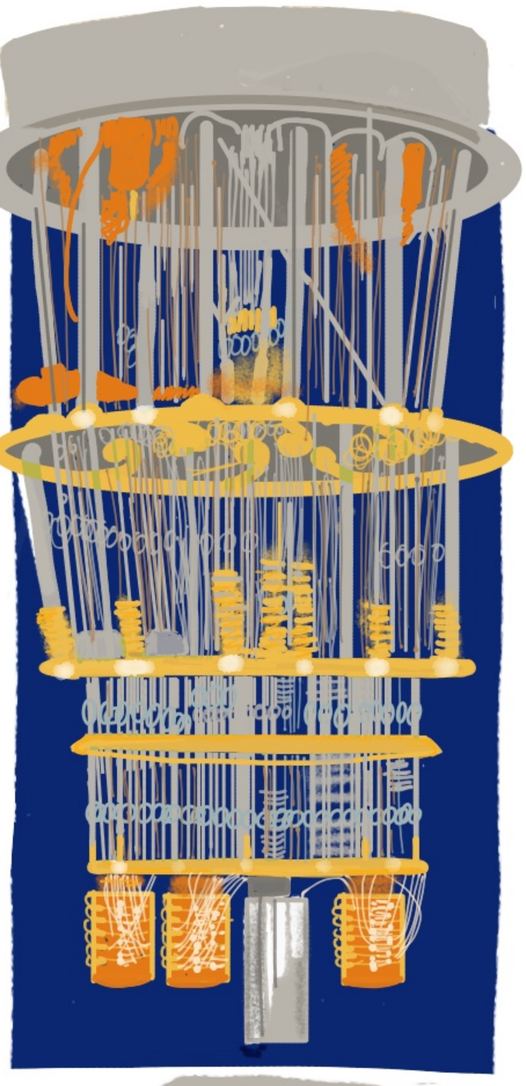
1985

Quantum theory, Church Turing Principle & Universal Quantum Computer

by

DAVID DEUTSCH

# WHAT IS IT MADE OF?



QUANTUM COMPUTER

**QUANTUM PARTICLES**

also called

**QUBITS**

such as

ELECTRONS/PHOTONS

whose **SPIN**
or **POLARISATION**

can be in

**SUPERPOSITION**

and a handful
are **ENTANGLED**

**QUANTUM ALGORITHMS**

are procedures using

**QUANTUM LOGIC GATES**

on quantum particles

to get

**COMPUTATION SPEED UP**

exploring several options
simultaneously

ending in a

**MEASUREMENT**

with a high

**PROBABILITY**

**SPECIALISED HARDWARE**

at **COLD COLD** temperatures

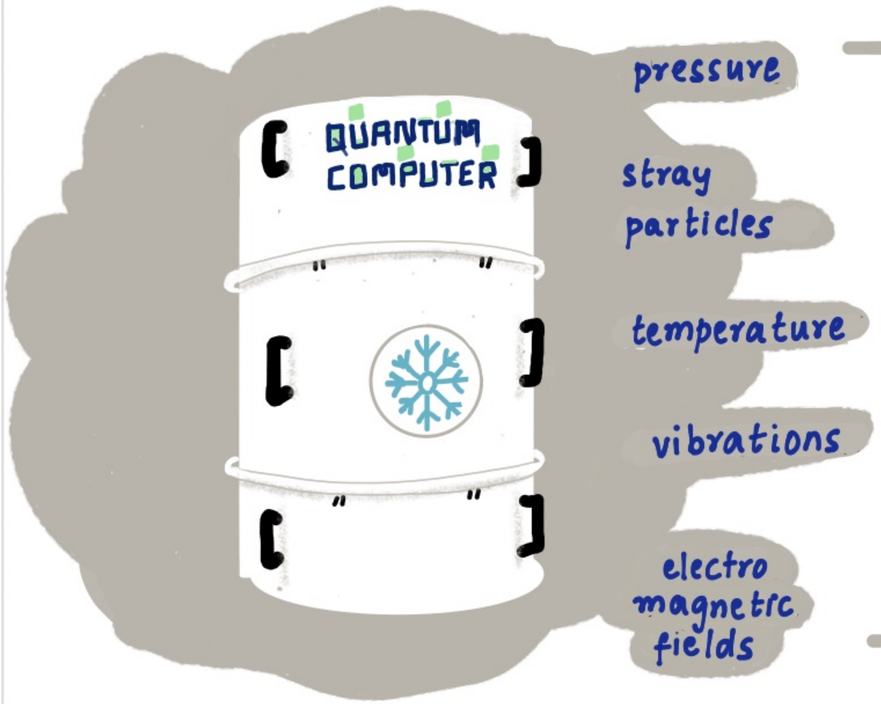
to **slow down**
quantum particles
manipulated by

MICROWAVE PULSES
in a **superconducting**
quantum computer

**OR**

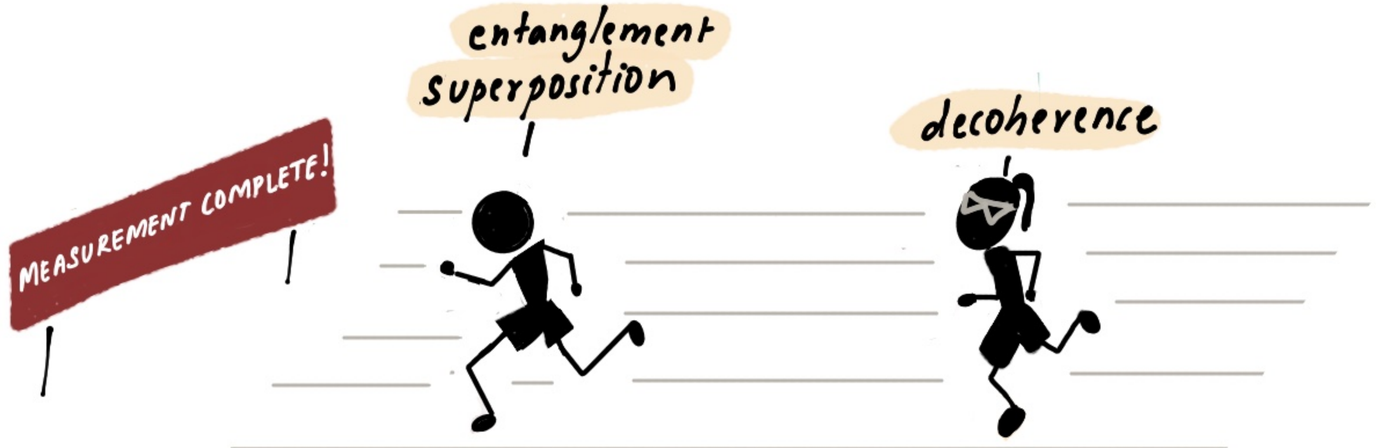
LASER BEAMS
in a **trapped-ion**
quantum computer

# DECOHERENCE : HARD TO KEEP QUANTUM




A QUANTUM SYSTEM HAS TO BE ISOLATED FROM ITS SURROUNDINGS TO KEEP QUANTUM BEHAVIOUR






$ $ THIS IS AN EXPENSIVE PROCESS $ $

ANY EXPOSURE TO 'NOISE' LEADS TO LOSS OF QUANTUMNESS - THIS IS CALLED DECOHERENCE

QUANTUM COMPUTERS ARE EXPONENTIALLY POWERFUL

— FROM THE SHEER AMOUNT OF INFORMATION IT CAN POTENTIALLY HOLD/PROCESS —

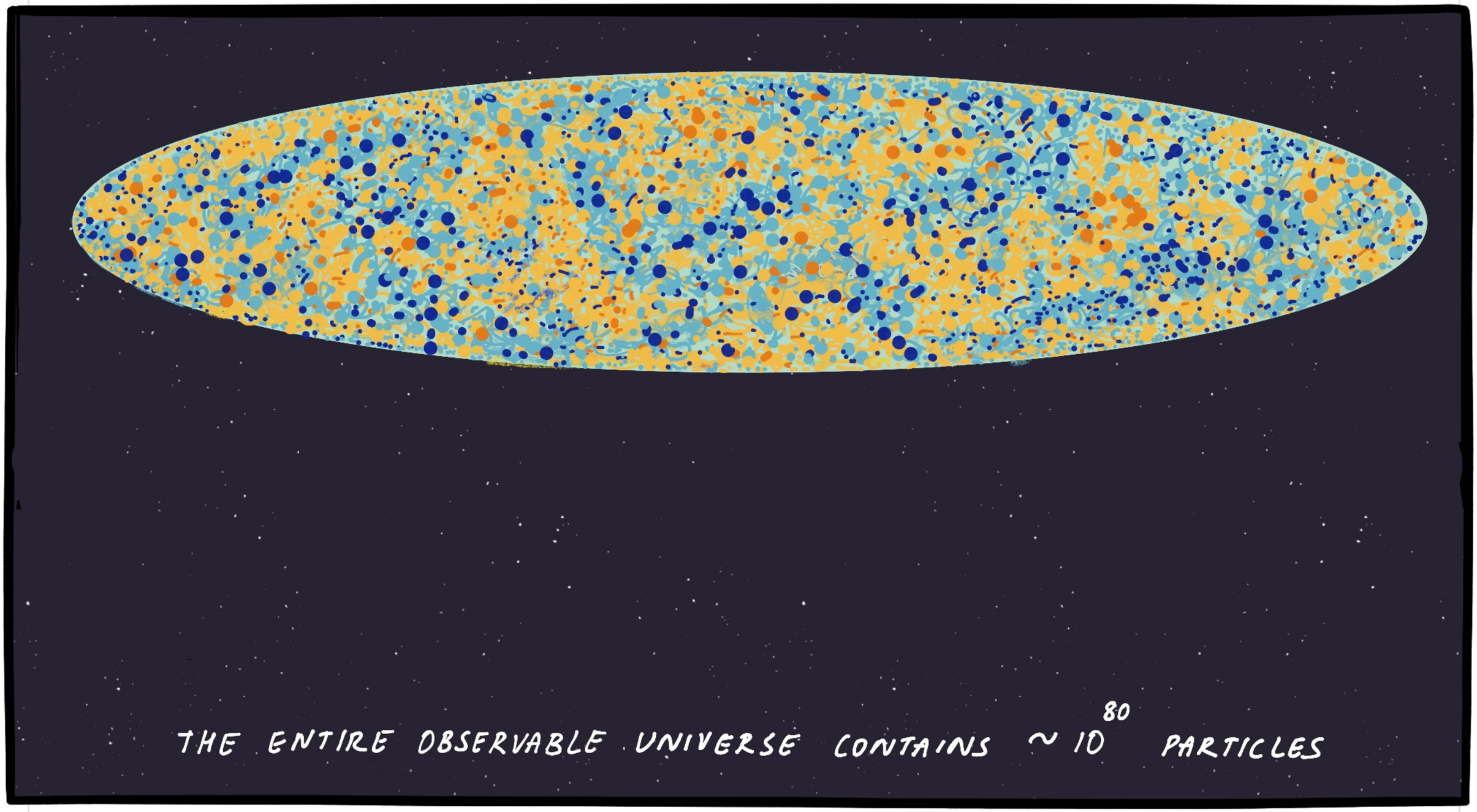
# 100 QUBITS




100 QUBITS CAN REPRESENT ~ $10^{30}$ STATES

Source: European Space Agency

# 300 QUBITS




300 QUBITS CAN REPRESENT ~ $10^{90}$ STATES

Source: Numberphile

# QUANTUM BITS

— KEEPERS OF THE INFORMATION —

WITH MUCH GRATITUDE TO UMESH VAZIRANI / UC BERKELEY

# A NOTE ON THE MATHEMATICS

AN INDEPTH STUDY OF QUANTUM COMPUTATION REQUIRES SOME KNOWLEDGE OF:

- PROBABILITY THEORY
- LINEAR ALGEBRA
- VECTORS/MATRICES/EIGENSTUFF/TENSOR PRODUCTS
- BIG O NOTATION
- PHYSICS

THAT IS NOT THE GOAL OF THIS BOOK. WE WILL INSTEAD DRAW CONVENIENTLY FROM HIGH SCHOOL MATHEMATICS.

- MULTIPLY ALGEBRAIC EXPRESSIONS
- RECOGNISE PYTHAGORAS' THEOREM
- KNOW REAL & IMAGINARY NUMBERS AND ABSOLUTE VALUES
- UNDERSTAND EXPONENTS/POWERS

BEING FAMILIAR WITH HOW A COMPUTER CAN BE PROGRAMMED IS ESSENTIAL. ANY OTHER SYMBOLS OR CONCEPTS WILL BE EXPLAINED AS WE GO ALONG

# BIT & QUBIT

## A BIT* IS A...

... BINARY DIGIT IN ONLY ONE OF TWO STATES

0

1

*named by Claude Shannon, 1940s

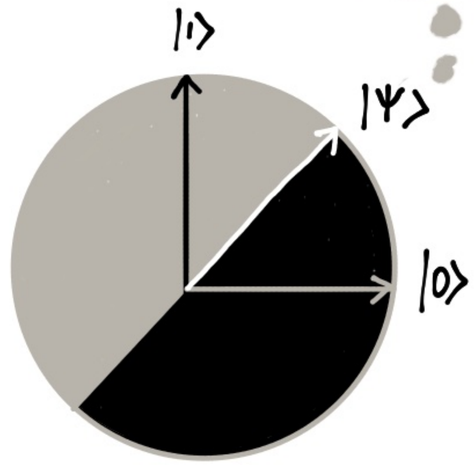
## A QUBIT IS A...

Greek letter psi

... QUANTUM BIT IN A SUPERPOSITION $\Psi$ OF

0 → to some extent

1 → to some other extent




*named by Benjamin Schumacher, 1990s

## TWO QUBITS

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| Q1 | 0 | 0 | 1 | 1 |
| Q2 | 0 | 1 | 0 | 1 |

can represent 4 possible states each with a certain likelihood

## THREE QUBITS

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| Q1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 |
| Q2 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| Q3 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 |

can represent 8 possible states each with a certain likelihood

# QUBITS AND STATES

1 qubit

2 qubits

3 qubits

4 qubits

5 qubits

6 qubits

7 qubits

8 qubits

9 qubits

50 qubits

1,000,000,000,000,000 states

ADDING ONE MORE QUBIT

DOUBLES

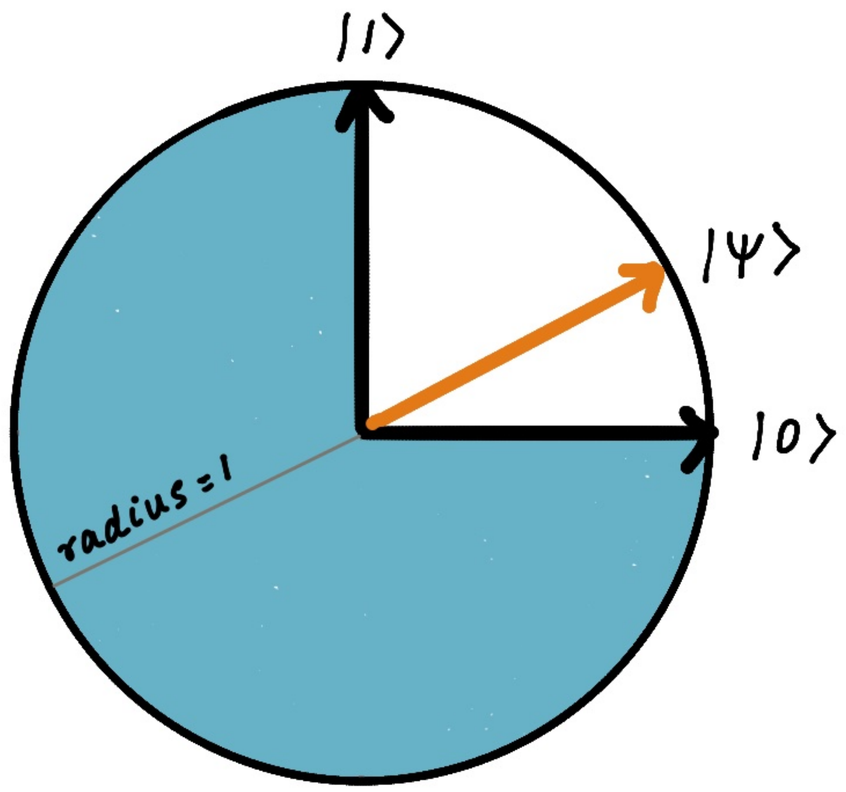
THE NUMBER OF POSSIBLE STATES

THIS INCREASE IS EXPONENTIAL

50

# MEET THE QUBIT

## GEOMETRIC VIEW OF THE QUBIT




MATHEMATICALLY, A QUBIT IS THE ARROW MARKED $\Psi$ (GREEK LETTER PSI) MOVING AROUND INSIDE A BALL OF RADIUS 1 UNIT

ALTOGETHER CALLED A BLOCH SPHERE

## BASIS

A QUBIT EXISTS RELATIVE TO THE BASIS STATES $|0\rangle$ AND $|1\rangle$

## QUANTUM STATES

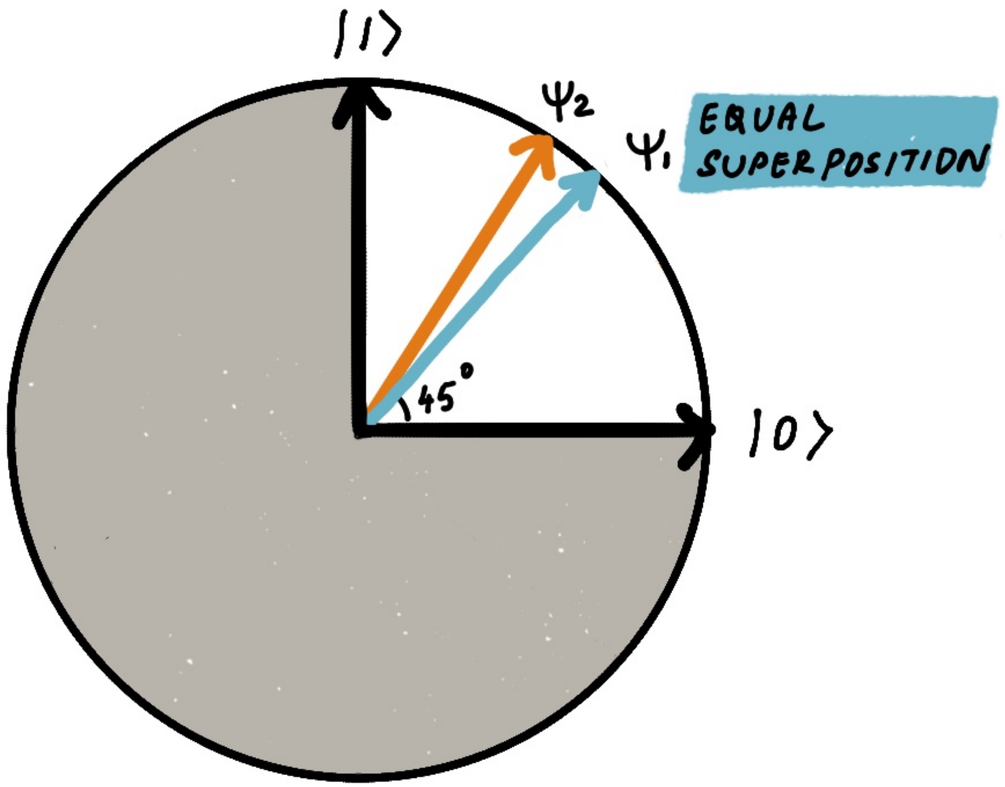
| | |
|---|---|
| $\|0\rangle$ | GROUND STATE / DOWN STATE |
| $\|1\rangle$ | EXCITED STATE / UP STATE |
| $\|\Psi\rangle$ | QUBIT STATE |

## NOTATION

THE BAR + BRACKET $|\ \rangle$ IS THE KET NOTATION CREATED BY THE PHYSICIST PAUL DIRAC

# QUBIT SUPERPOSITION

## GEOMETRIC VIEW OF THE QUBIT




## A QUBIT STATE

✓ IS A SUPERPOSITION OF $|0\rangle$ AND $|1\rangle$

✗ IS NOT BOTH $|0\rangle$ AND $|1\rangle$

## SUPERPOSITION

"DESCRIBES TO WHAT EXTENT A QUBIT IS IN $|0\rangle$ OR IN $|1\rangle$"

-UMESH VAZIRANI

Superposition

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

where

$\alpha, \beta$ are complex numbers

## AMPLITUDES

"PRE-PROBABILITIES"

- SCOTT AARONSON

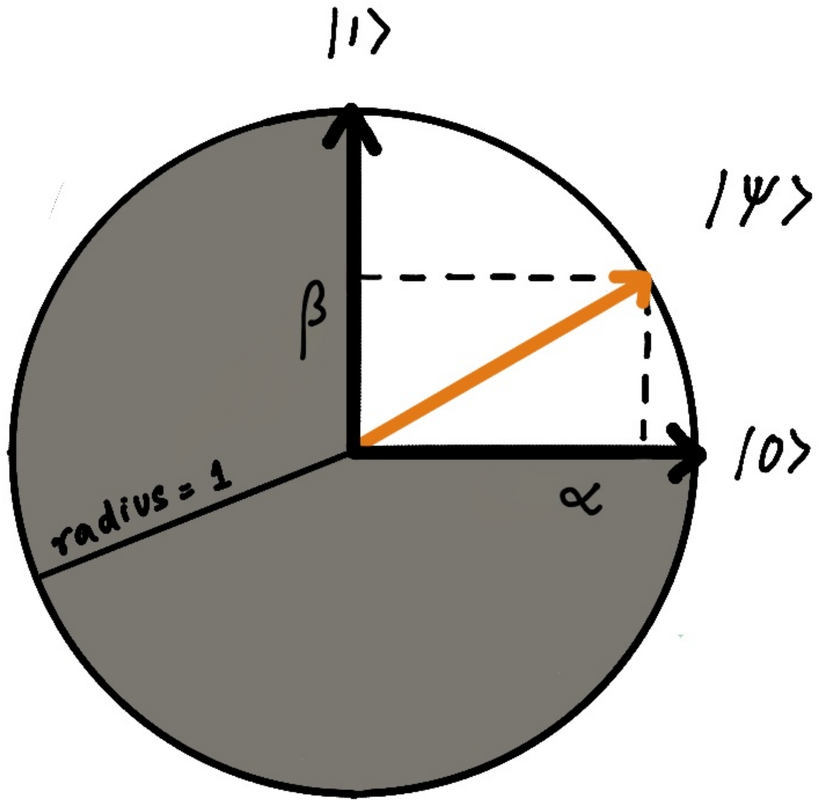
## EQUAL SUPERPOSITION

THE QUBIT IS EQUALLY LIKELY TO BE IN STATE $|0\rangle$ OR STATE $|1\rangle$

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

# QUBIT, MAKE UP YOUR MIND

## GEOMETRIC VIEW OF THE QUBIT




SUPERPOSITION OF A QUBIT IS $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

## AMPLITUDE

$\alpha$ = AMPLITUDE OF $|0\rangle$

$\beta$ = AMPLITUDE OF $|1\rangle$

## MEASUREMENT

WHEN A QUBIT IS MEASURED, ITS SUPERPOSITION 'COLLAPSES'

IT CHOOSES A STATE $|0\rangle$ OR $|1\rangle$

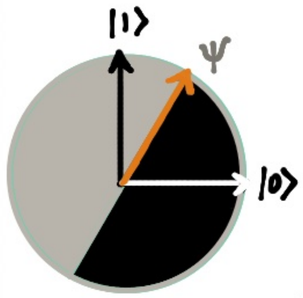
## PROBABILITIES OF OUTCOMES

PROBABILITY OF $|0\rangle = |\alpha|^2$

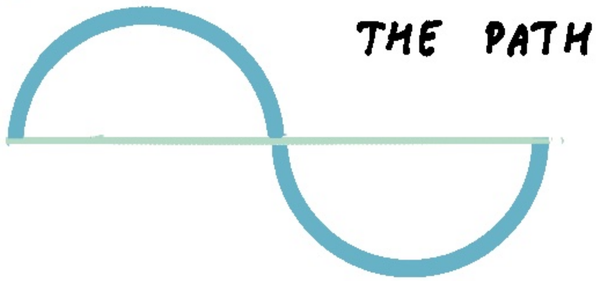
PROBABILITY OF $|1\rangle = |\beta|^2$

$$|\alpha|^2 + |\beta|^2 = 1$$

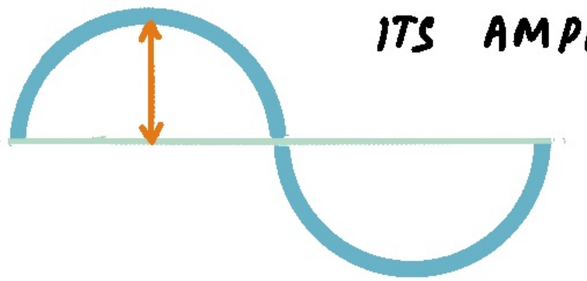
# FROM SUPERPOSITION TO DEFINITE POSITION



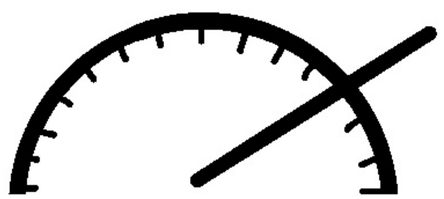

THE QUBIT GOES ROUND THE CIRCLE



THE PATH IT TRACES IS REALLY A WAVE

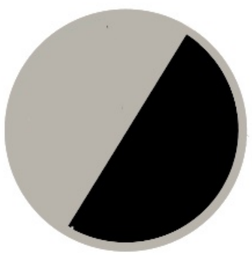


ITS AMPLITUDE DETERMINES THE PROBABILITY OF THE OUTCOME (zero or one)

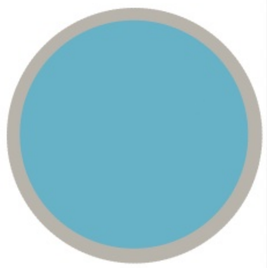


MEASURING THE QUBIT CHANGES THE AMPLITUDE TO A PROBABILITY

THE HIGHER THE PROBABILITY THE MORE LIKELY THE OUTCOME



LET US TAKE A CLOSER LOOK AT THE JOURNEY FROM QUBIT TO BIT

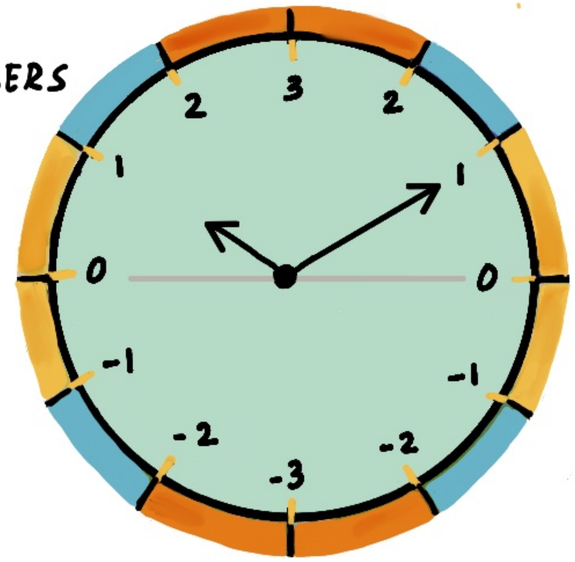


# WHAT GOES AROUND IS A WAVE

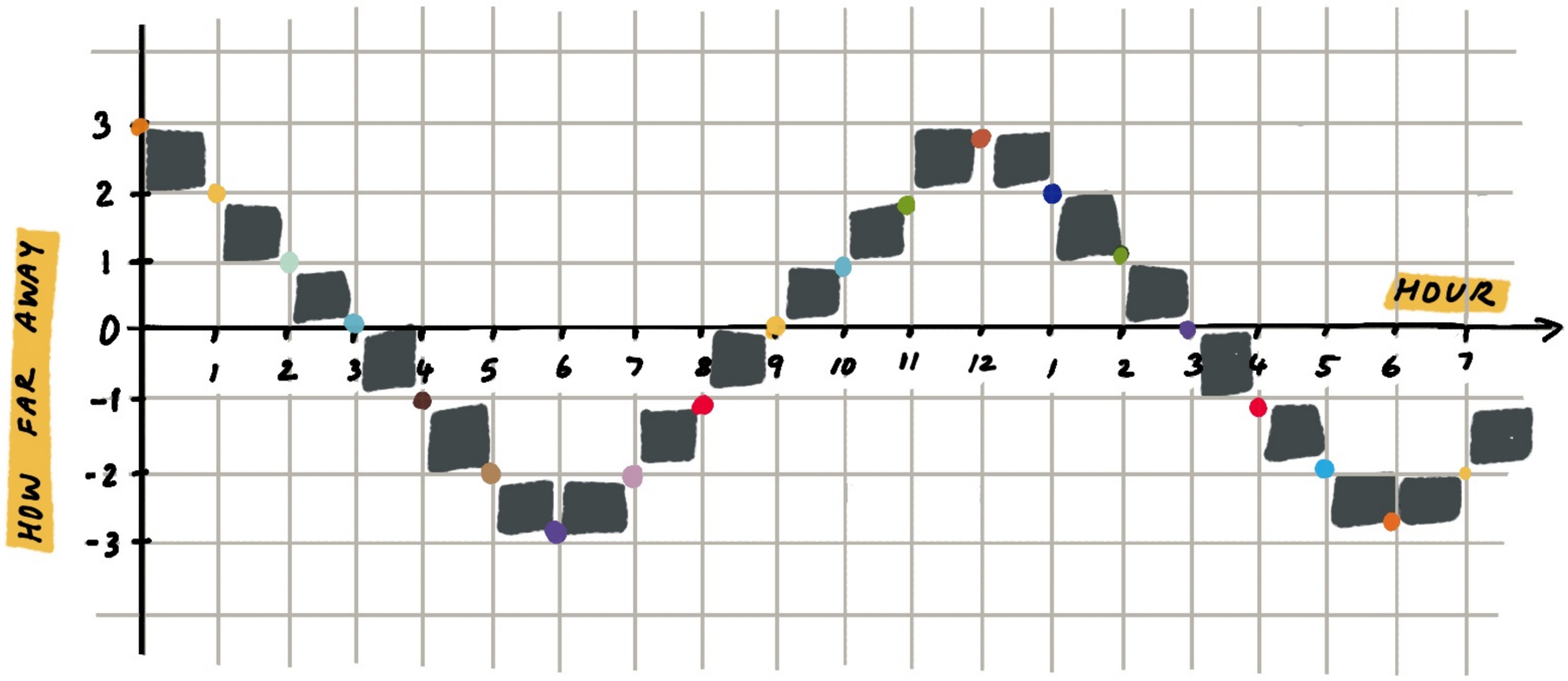
1. TAKE A REGULAR CLOCK




2. REPLACE ALL NUMBERS WITH HOW FAR AWAY THEY ARE FROM THE HORIZONTAL



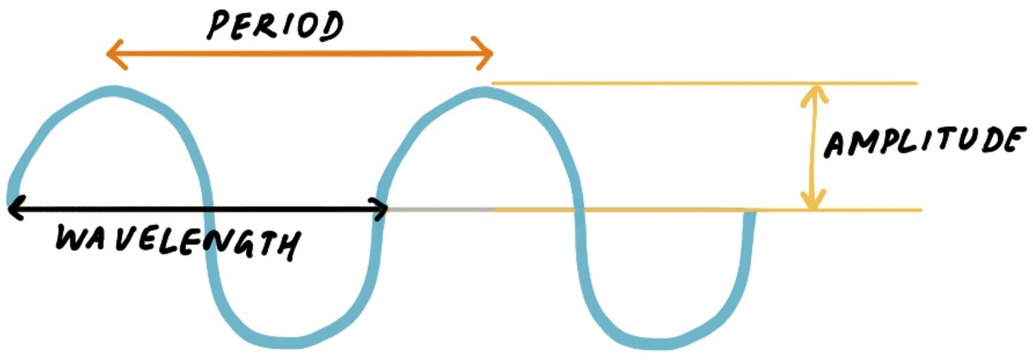

3. PLOT HOW FAR AWAY FROM ZERO THE HOUR HAND TRAVELS AFTER 12:00



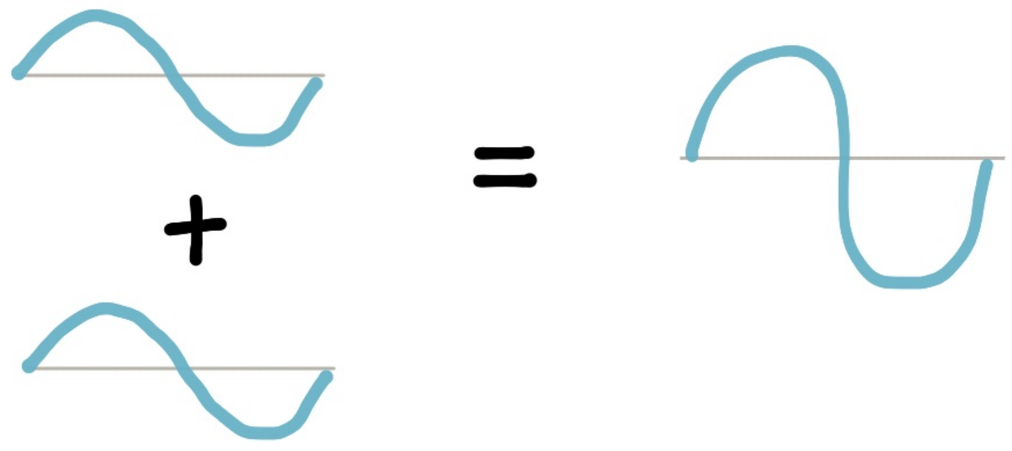

SEE A WAVE PATTERN FORMING

# ABOUT AMPLITUDES

## AMPLITUDE IS A PROPERTY OF WAVES

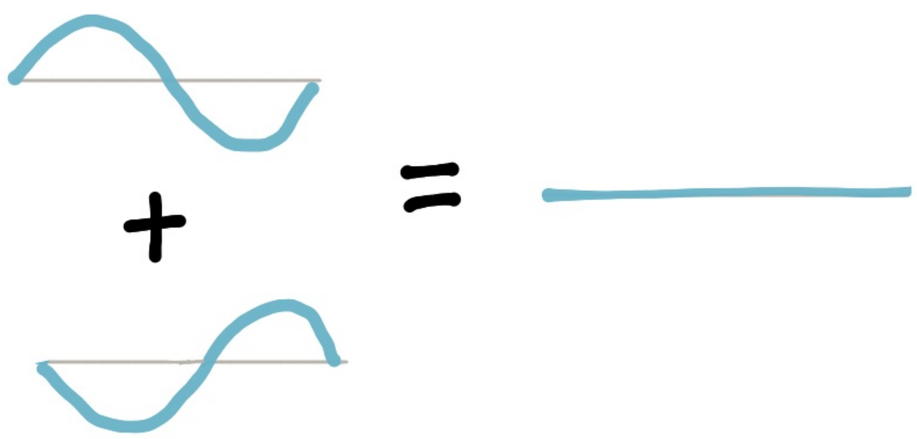



## AMPLITUDES ADD UP



WHEN WAVES PASS EACH OTHER, THEY INTERFERE

## AMPLITUDES CANCEL EACH OTHER



## AMPLITUDES INFLUENCE OUTCOMES

THIS INTERFERENCE CAN BE USED

- TO CANCEL WRONG ANSWERS
- TO AMPLIFY CORRECT ANSWERS

WITH A HIGH PROBABILITY

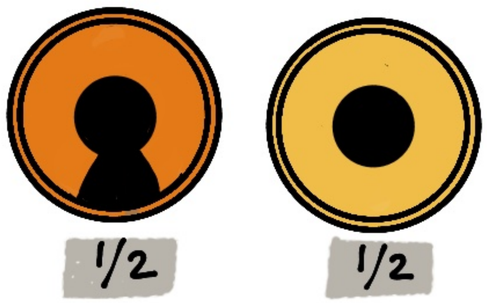
AMPLITUDE — becomes — PROBABILITY

# PROBABILITY vs AMPLITUDE

## COIN STATES

A COIN FLIP ENDS IN HEADS OR TAILS

REAL WORLD OUTCOMES HAVE PROBABILITIES




PROBABILITIES ARE REAL NUMBERS SUCH AS

0, 0·5, 2/3, 0·777, 1

. . . NEVER NEGATIVE

SUM OF PROBABILITIES = 1

SUM OF PROBABILITIES

$$\left(\frac{1}{2}\right) + \left(\frac{1}{2}\right) = 1$$

## QUBIT STATES

A QUBIT $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ ENDS IN $|0\rangle$ OR $|1\rangle$

QUANTUM WORLD OUTCOMES HAVE AMPLITUDES




AMPLITUDES CAN BE POSITIVE, NEGATIVE OR COMPLEX NUMBERS

. . . ENABLING THEM TO INTERFERE

SUM OF PROBABILITIES = 1

$|\text{AMPLITUDE}|^2 = \text{PROBABILITY}$

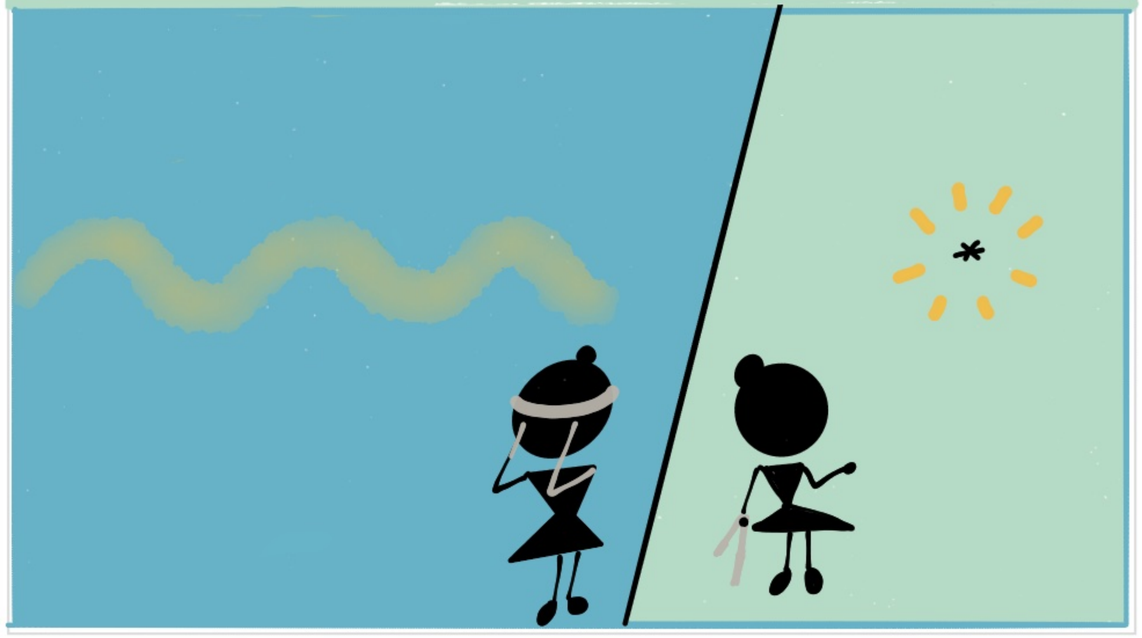
IF AMPLITUDES $\alpha = \frac{1}{\sqrt{2}}$ $\beta = \frac{1}{\sqrt{2}}$, THEN

SUM OF PROBABILITIES

$$\left|\frac{1}{\sqrt{2}}\right|^2 + \left|\frac{1}{\sqrt{2}}\right|^2 = 1$$

# MEASUREMENT

CHANGES AN AMPLITUDE TO PROBABILITY

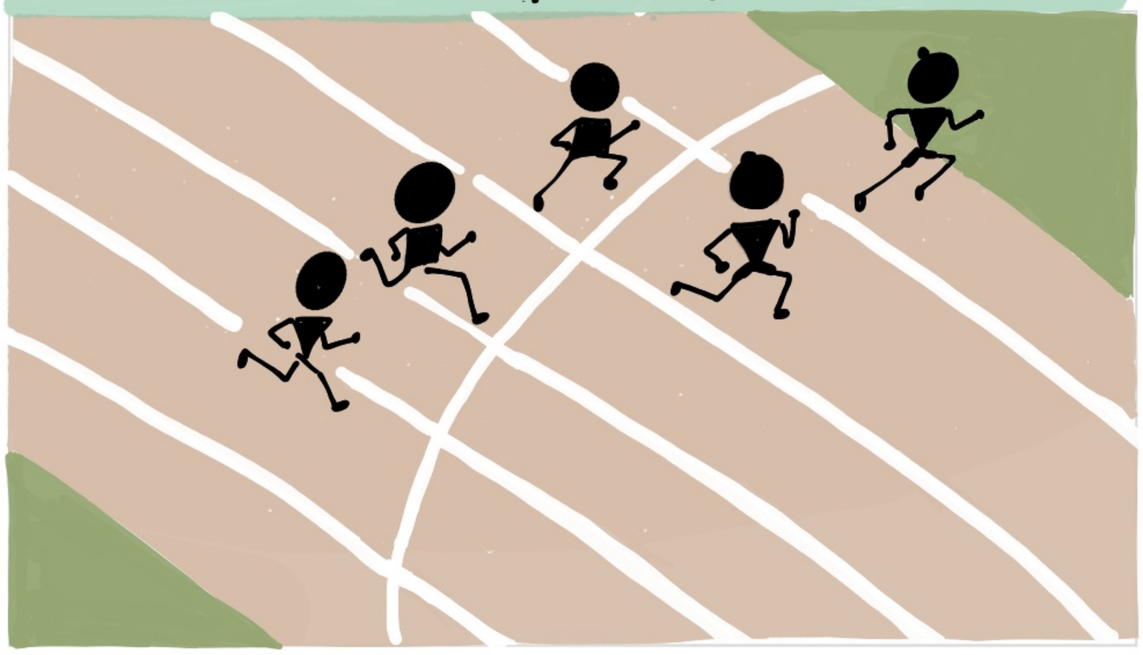


ALTERS WHAT IS BEING MEASURED

IT FORCES THE QUBIT
TO MAKE A DECISION

IT LOSES THE SUPERPOSITION

DESCRIBES A STATE / POSITION



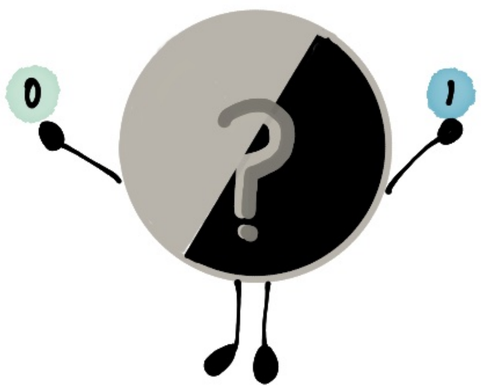
GIVES A RANDOM ANSWER

... DEPENDING ON THE PROBABILITY

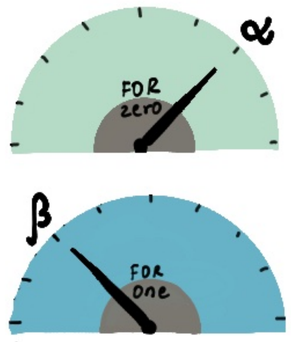


# A RANDOM ANSWER IS NO GOOD

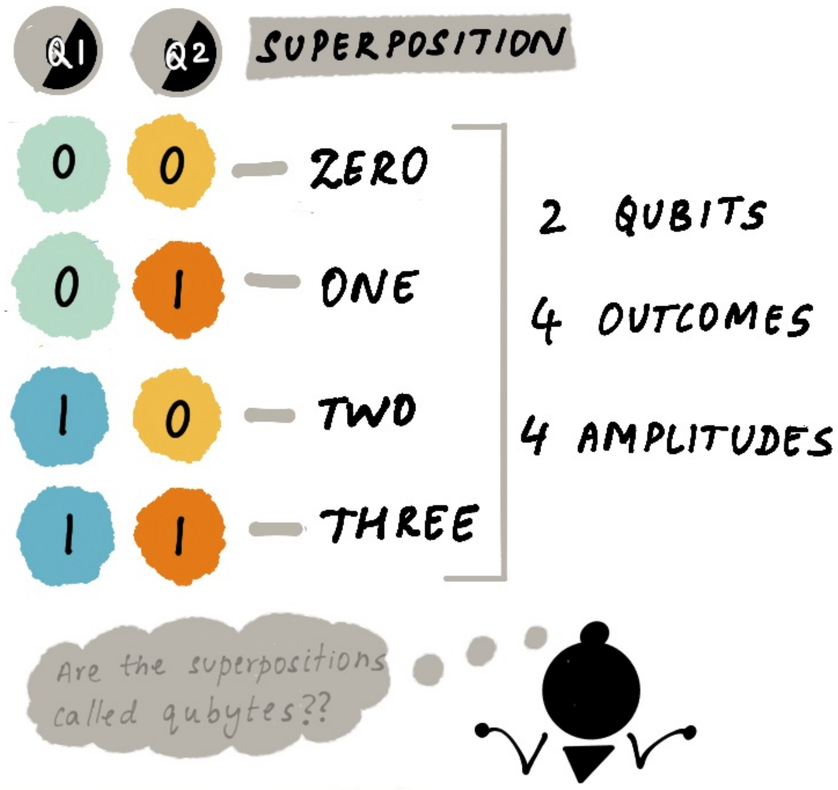
HOWEVER, A QUANTUM COMPUTER CAN BE COAXED INTO A MORE LIKELY ANSWER




EVERY QUBIT HAS
2 POTENTIAL OUTCOMES




EVERY OUTCOME
HAS AN AMPLITUDE






AMPLITUDES
CAN BE
CONTROLLED
BY RULES (OR GATES)

THIS MAKES THEM ...

... INTERFERE
AND CANCEL OUT
THE UNWANTED
ONES




(HANDY THAT AMPLITUDES CAN
BE NEGATIVE / COMPLEX)

THE RULES WORK
TOGETHER IN A
QUANTUM ALGORITHM
(OR QUANTUM CIRCUIT)

SO ...

# A LIKELY CORRECT ANSWER

A QUANTUM — ALGORITHM

IS MADE UP OF — GATES | RULES

WHICH — MANIPULATE AMPLITUDES OF QUBITS

SUCH THAT

WHEN AMPLITUDES — INTERFERE

THE AMPLITUDES OF

THE WRONG ANSWERS — CANCEL EACH OTHER

THE AMPLITUDES OF

THE RIGHT ANSWERS — ADD UP AND AMPLIFY

SO, ON — MEASUREMENT

WE FIND — UNDESIRED OUTCOMES LESS PROBABLE

CORRECT ANSWERS MORE LIKELY

# GATES: A MEANS TO CALCULATE

# CLASSICAL LOGIC GATES

ELECTRONIC CIRCUITS USE LOGIC GATES TO PERFORM CALCULATIONS



RATHER LIKE GATES,
NOT ALL GET THROUGH

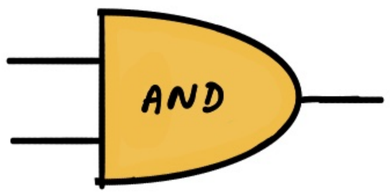



ONE OR TWO STATEMENTS
ARE EXAMINED AT EACH GATE

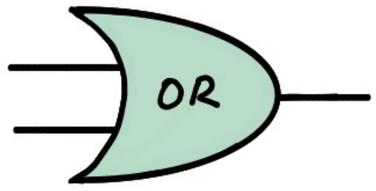


WHAT PASSES DEPENDS ON
THE RULES OF THE GATE

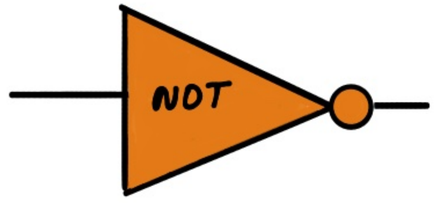
THESE THREE GATES FORM THE BASIS OF ALL CALCULATIONS




PASSES TRUE ONLY IF
BOTH STATEMENTS ARE TRUE




PASSES TRUE IF ONE
OF TWO STATEMENTS IS TRUE




PASSES THE OPPOSITE
OF THE STATEMENT

# QUANTUM LOGIC GATES

## BIT FLIP

BEHAVES LIKE A NOT-GATE

## PHASE FLIP

CHANGES THE SIGN OF $|1\rangle$

## HADAMARD

ACHIEVES EQUAL SUPERPOSITION

## CNOT

FLIPS SECOND IF FIRST IS 1

QUBITS OBEY RULES IN AN ALGORITHM

THESE RULES ARE CALLED GATES

GATES ARE APPLIED TO ONE OR MORE QUBITS AT A TIME

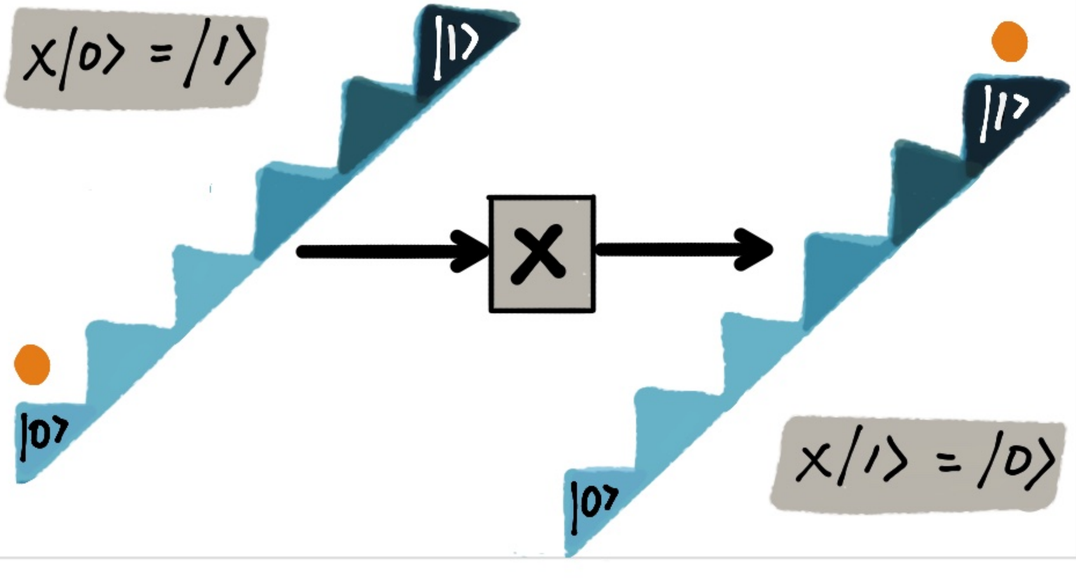
THE GATES MAKE QUBITS MOVE AROUND THE BLOCH SPHERE

THIS CHANGES THE AMPLITUDES OF EACH OUTCOME OF THE QUBITS

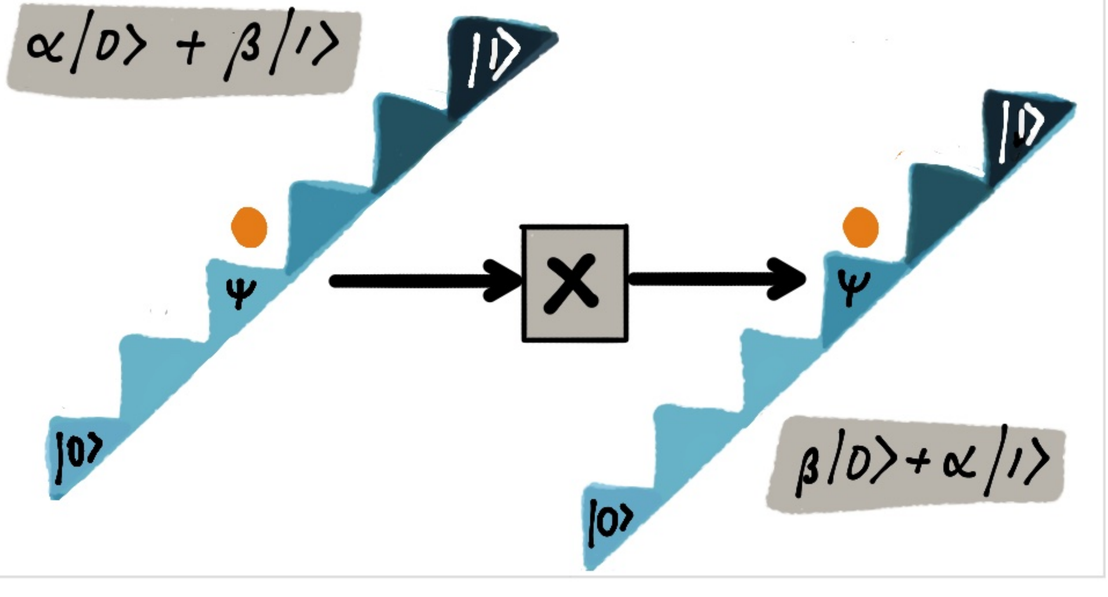
OBVIOUSLY, THERE ARE OTHER GATES, BUT THESE FOUR ARE GOOD FOR A START

# BIT FLIP GATE (X)

## IT IS A QUANTUM NOT-GATE



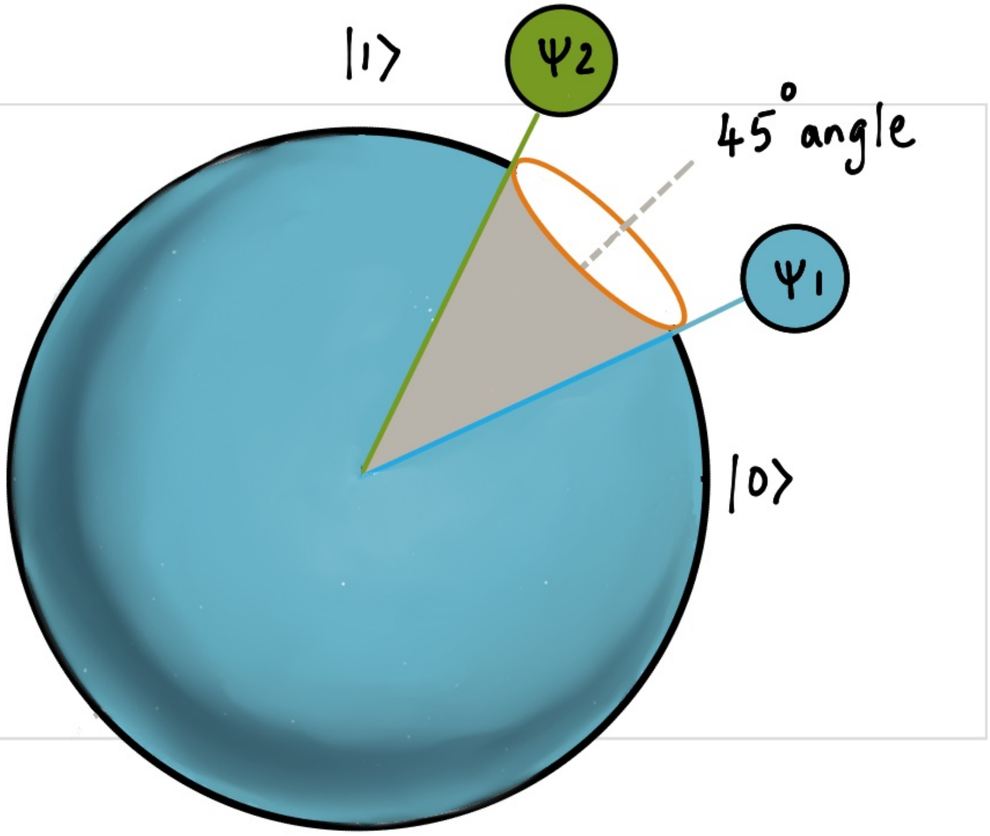

## FOR A QUBIT IN SUPERPOSITION




## ROTATION ABOUT THE 45° AXIS

A BIT FLIP IS A HALF-CIRCLE ROTATION
AROUND THE 45° ANGLE
TO GO FROM STATE $\Psi_1$ TO $\Psi_2$

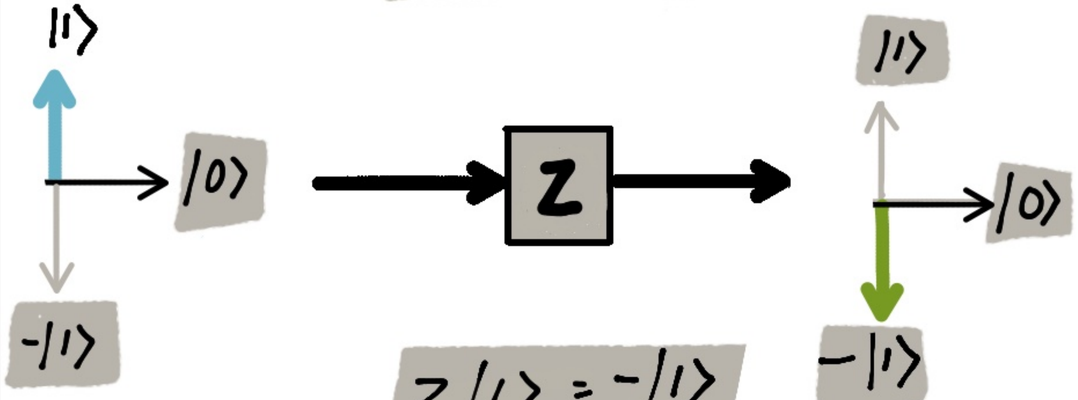
DO THE BIT FLIP TWICE AND
WE ARE BACK TO WHERE WE STARTED



# PHASE FLIP GATE (Z)

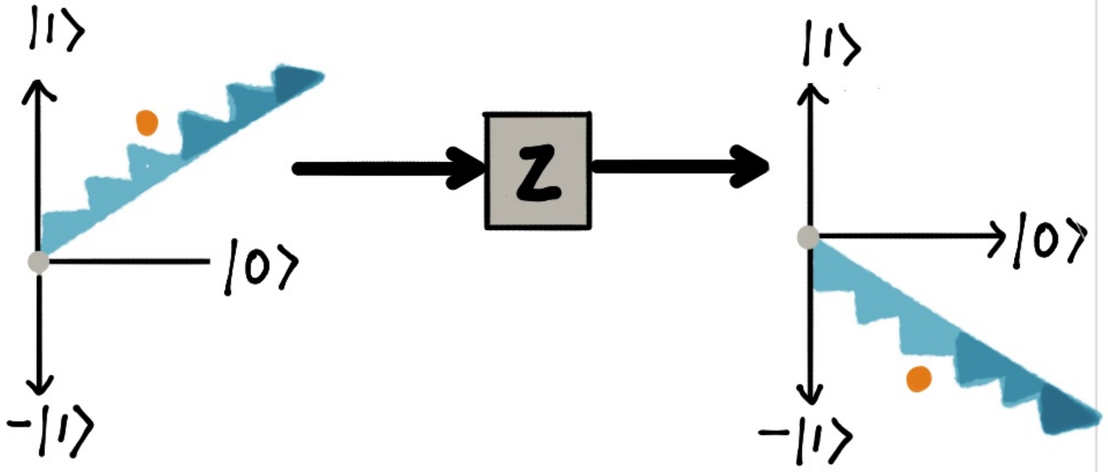
## IT IS A PHASE (SIGN) CHANGE GATE

$Z|0\rangle = |0\rangle$




$Z|1\rangle = -|1\rangle$

## FOR A QUBIT IN SUPERPOSITION



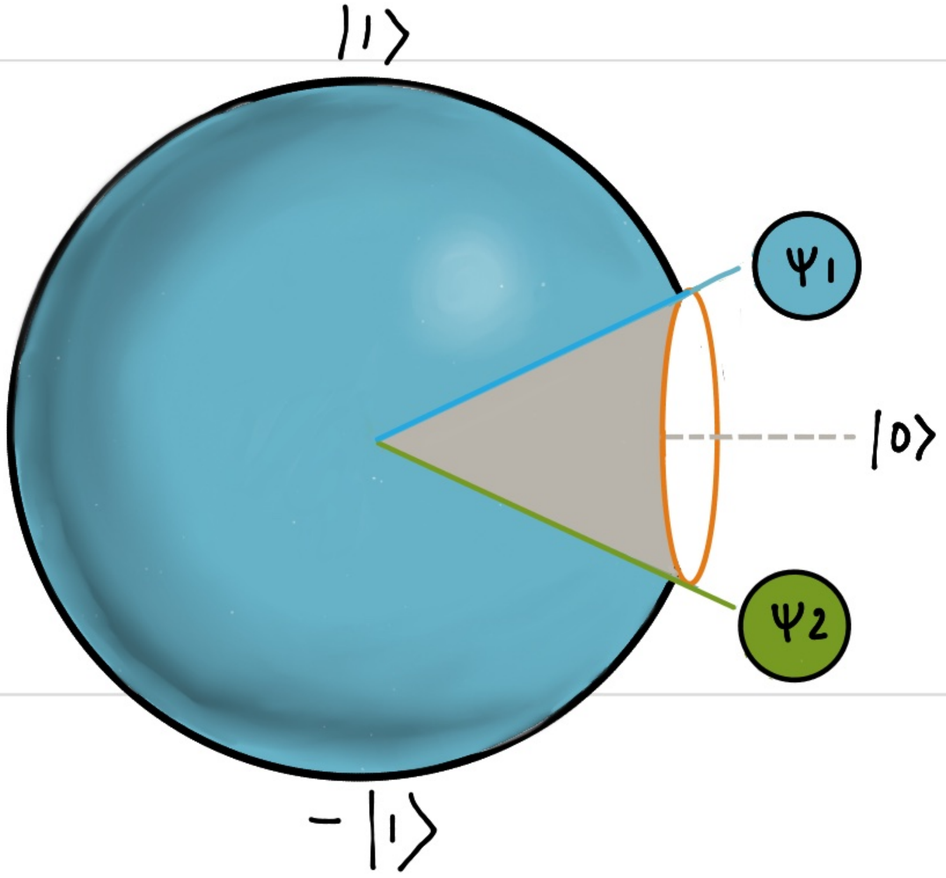

$\alpha|0\rangle + \beta|1\rangle$ $\alpha|0\rangle - \beta|1\rangle$

## ROTATION ABOUT THE $|0\rangle$ AXIS

A PHASE FLIP IS A HALF-CIRCLE ROTATION AROUND THE $|0\rangle$ STATE

TO GO FROM STATE $\Psi_1$ TO $\Psi_2$

DO THE PHASE FLIP TWICE AND WE ARE BACK TO WHERE WE STARTED



# HADAMARD GATE (H)

## PUTS QUBITS IN EQUAL SUPERPOSITION

$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = |+\rangle$

$|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = |-\rangle$

$|+\rangle, |-\rangle$ ARE AT 90°

## FOR A QUBIT IN SUPERPOSITION

$H(\alpha|0\rangle + \beta|1\rangle)$

$= \alpha\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) + \beta\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)$

$= \frac{1}{\sqrt{2}}(\alpha|0\rangle + \alpha|1\rangle + \beta|0\rangle - \beta|1\rangle)$

$= \frac{1}{\sqrt{2}}(\alpha+\beta)|0\rangle + \frac{1}{\sqrt{2}}(\alpha-\beta)|1\rangle$

= CREATES A NEW SUPERPOSITION

## ROTATION ABOUT THE 22.5° AXIS

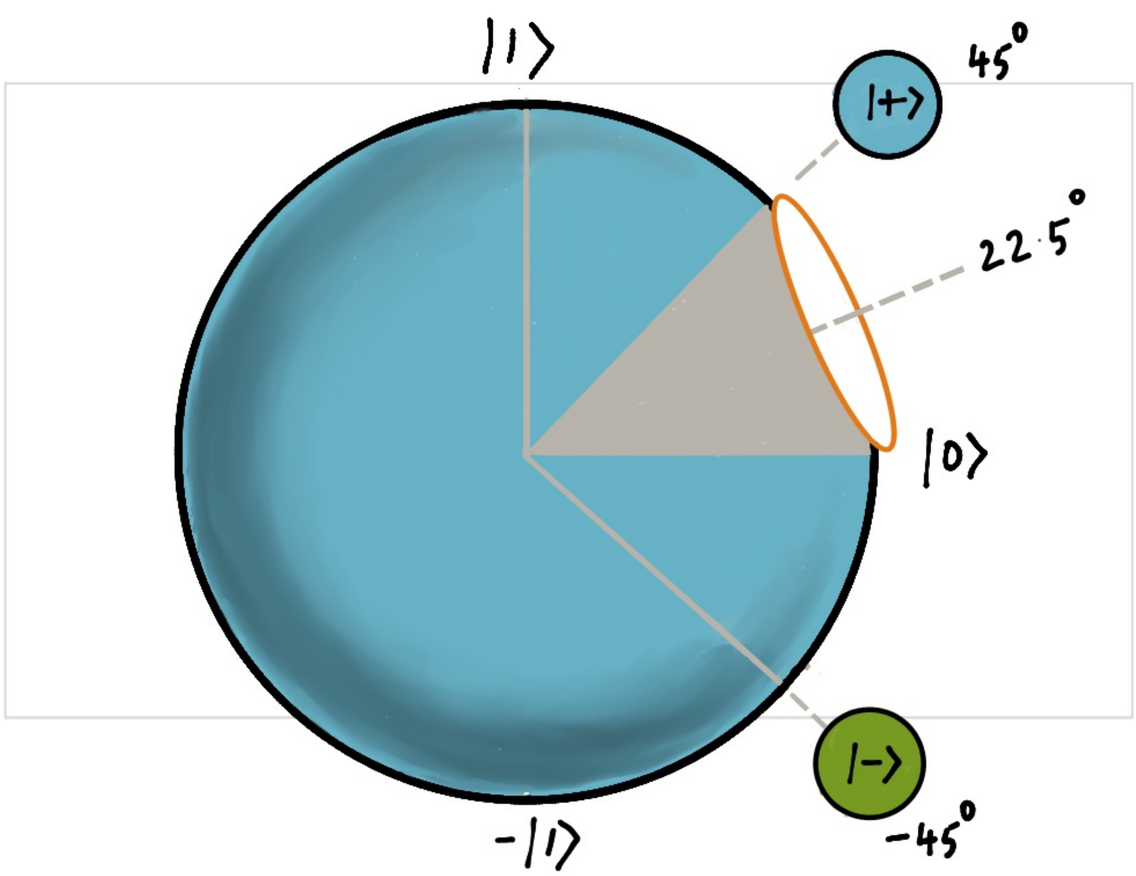
A HADAMARD IS A HALF-CIRCLE ROTATION AROUND THE 22.5° ANGLE TO GO

FROM $|0\rangle$ TO $|+\rangle$

OR

FROM $|1\rangle$ TO $|-\rangle$

DO THE HADAMARD TWICE AND WE ARE BACK TO WHERE WE STARTED

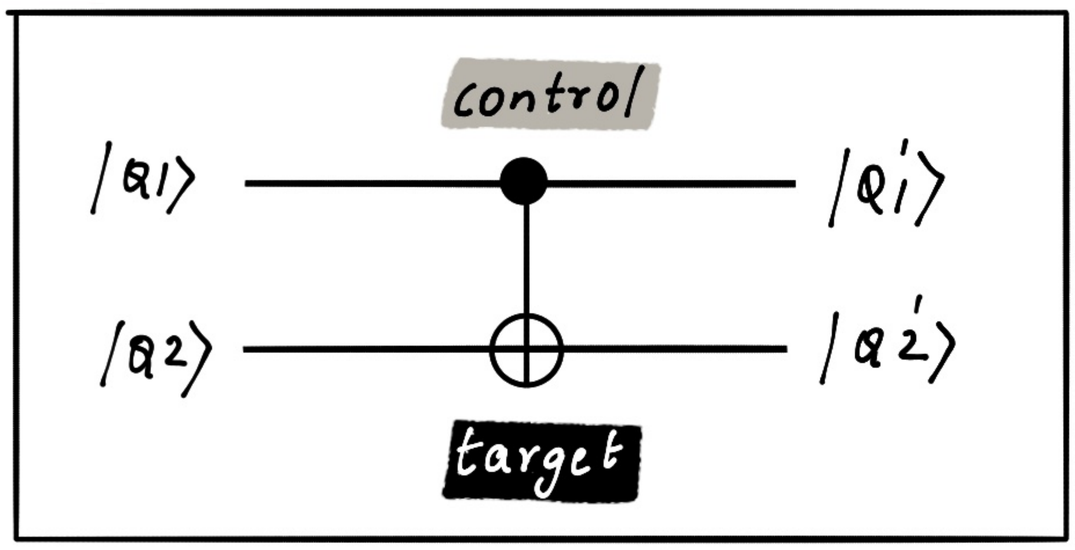


# CNOT GATE

THE **CONTROLLED NOT** CNOT GATE ACTS ON TWO QUBITS

FLIPS THE SECOND QUBIT IF THE FIRST QUBIT IS 1

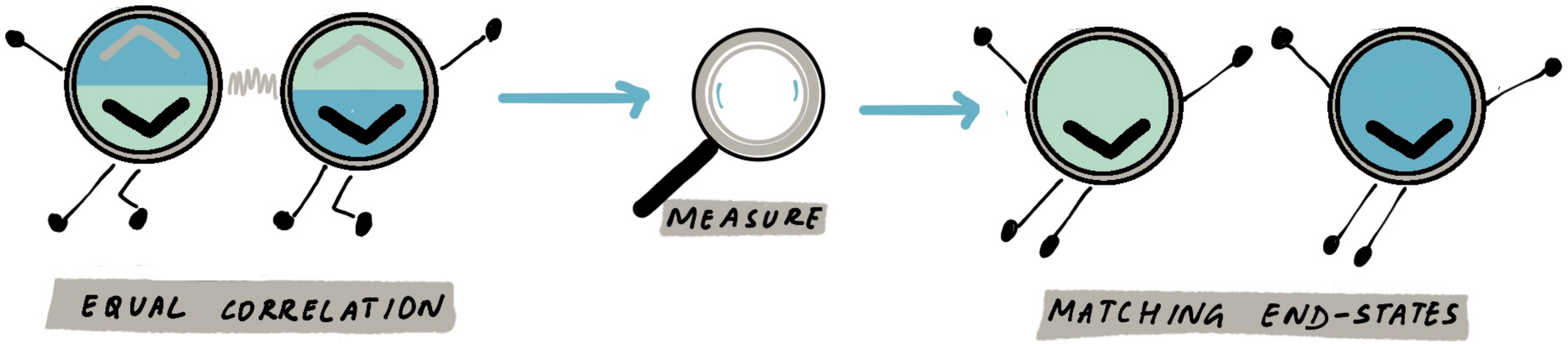
**Quantum circuit**




| Q1 | Q2 | CNOT |
|---|---|---|
| 0 | 0 | 00 |
| 0 | 1 | 01 |
| 1 | 0 | 11 |
| 1 | 1 | 10 |

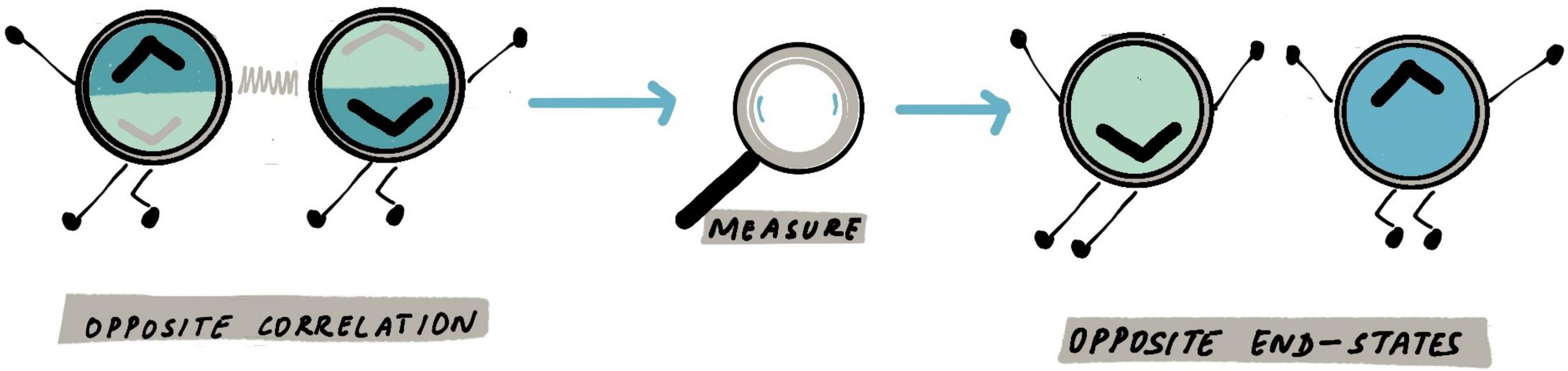
INTERESTINGLY, THE CNOT GATE CAN BE USED TO CREATE ENTANGLED QUBITS

# ENTANGLEMENT - A RECAP

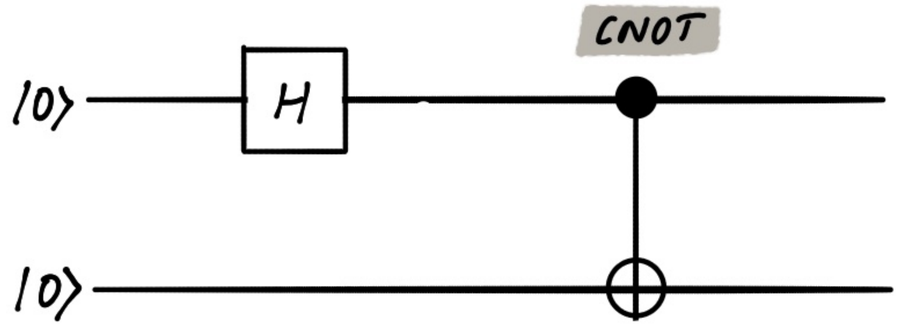



PROPERTIES OF ENTANGLED QUBITS CAN ONLY BE DESCRIBED AS A WHOLE - NOT INDIVIDUALLY

MEASURING ONE AFFECTS/DECIDES THE STATE OF THE OTHER EVEN IF THE TWO ARE LIGHT YEARS APART



# GATES FOR ENTANGLEMENT




INITIAL STATE = $|00\rangle$

HADAMARD ON $|0\rangle$ = $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

COMBINED STATE = $(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle)|0\rangle$

= $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$

CNOT ON $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$ = $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

A MATHEMATICAL DESCRIPTION OF THE ENTANGLED STATE

# ENTANGLEMENT IS STRANGE

TWO QUBITS ARE ENTANGLED WHEN THEY ARE IN AN EQUAL SUPERPOSITION OF $|00\rangle$ AND $|11\rangle$

MEASURE ONE QUBIT AND INSTANTLY...

| | |
|---|---|
| $\frac{1}{\sqrt{2}}\|00\rangle + \frac{1}{\sqrt{2}}\|11\rangle$ | $\frac{1}{\sqrt{2}}\|01\rangle + \frac{1}{\sqrt{2}}\|10\rangle$ |
| $\frac{1}{\sqrt{2}}\|00\rangle - \frac{1}{\sqrt{2}}\|11\rangle$ | $\frac{1}{\sqrt{2}}\|01\rangle - \frac{1}{\sqrt{2}}\|10\rangle$ |

..THIS DECIDES THE MEASURE OF THE OTHER QUBIT

THERE ARE 4 STATES OF ENTANGLEMENT CALLED BELL STATES - AFTER JOHN S. BELL

## THE STRANGE IMPLICATION OF A BELL STATE

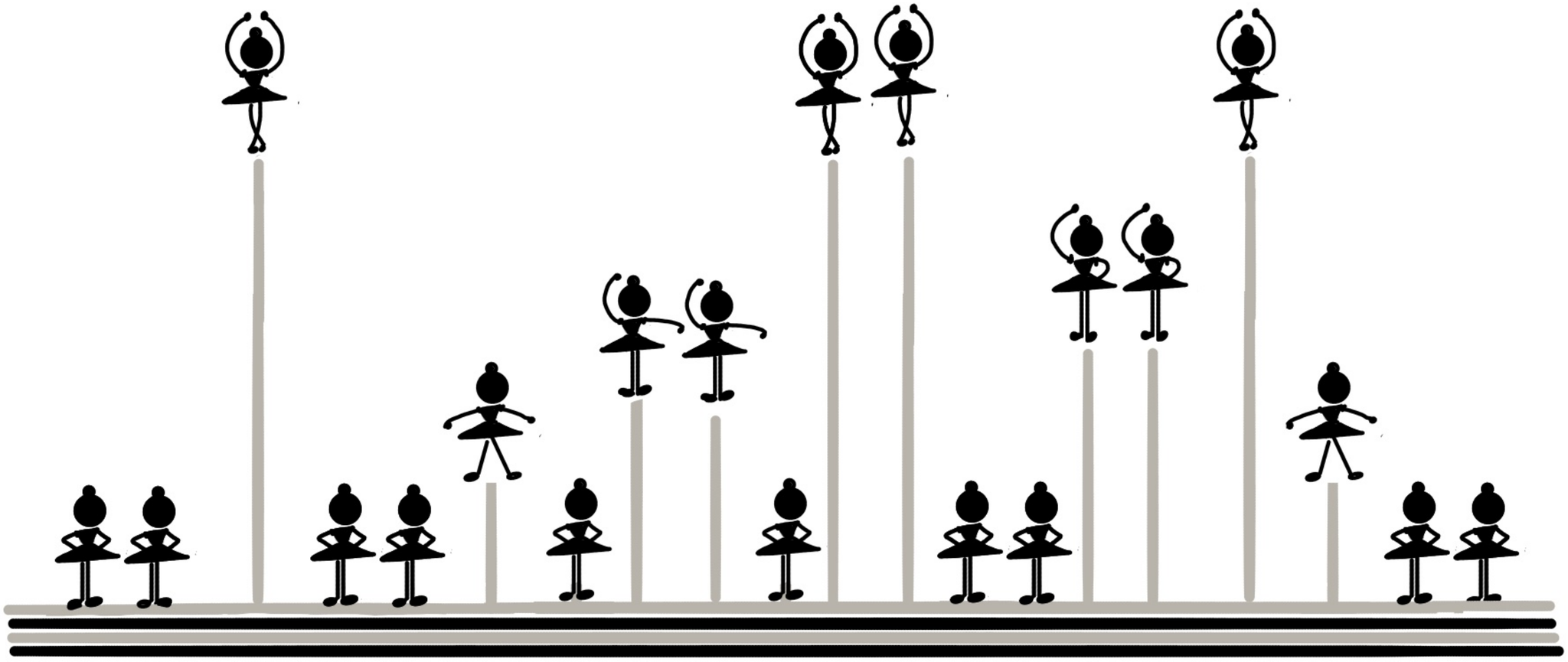
TAKE $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ : PROBABILITY OF FIRST QUBIT = 0 IS 50%.

IF THE FIRST QUBIT = 0, PROBABILITY OF SECOND QUBIT = 0 IS 100%.

# QUANTUM ALGORITHMS

## - A CONCEPTUAL MODEL -

# QUANTUM ALGORITHM - RECAP



A QUANTUM ALGORITHM USES A 'GLOBAL' PROPERTY OF THE VALUES IN THE QUBITS TO CHANGE THEIR AMPLITUDE.

GOAL
- REDUCE AMPLITUDE OF WRONG ANSWERS
- INCREASE AMPLITUDE OF CORRECT ANSWERS

SO, WHEN A MEASUREMENT IS MADE, THERE IS A HIGH PROBABILITY THAT THE ANSWER IS CORRECT

# HOW DO QUANTUM ALGORITHMS WORK?

IN CONTRAST TO CLASSICAL ALGORITHMS, THERE ARE ONLY A HANDFUL OF QUANTUM ALGORITHMS.

THEY APPEAR TO BE CAPABLE OF SOLVING HARDER PROBLEMS FASTER

THESE ALGORITHMS ARE COMPOSED AND EXECUTED VERY DIFFERENTLY FROM WHAT WE ARE USED TO IN CLASSICAL COMPUTERS

QUANTUM ALGORITHMS WORK BETTER ON PROBLEMS WITH A CERTAIN STRUCTURE TO PROVIDE SPEED UP. THE FIRST SUCH IS THE BERNSTEIN-VAZIRANI ALGORITHM

TO UNDERSTAND THEM A BIT BETTER, WE WILL LOOK A BIT CLOSELY AT THE WORKINGS OF THE :

- DEUTSCH-JOZSA ALGORITHM
- GROVER'S ALGORITHM
- SHOR'S ALGORITHM

EXERCISE : LOOKUP quantumalgorithm200.org

# DEUTSCH-JOZSA ALGORITHM

# DEUTSCH'S PROBLEM

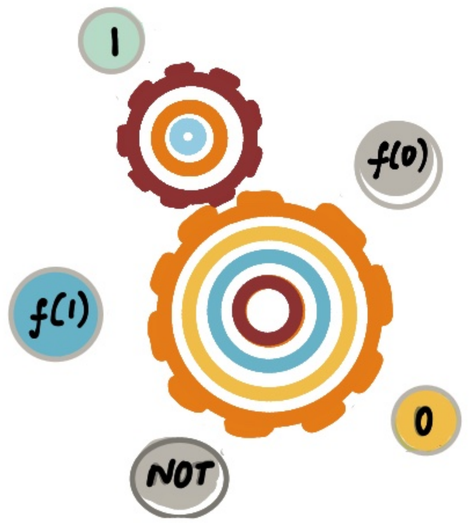
## THE PROBLEM : WHO AM I ?

I am a function f()

My input is a 0 or 1

My output is a 0 or 1

Am I constant or balanced ?




## AM I CONSTANT OR BALANCED ?

$f(x) = 0$ > CONSTANT OUTPUT

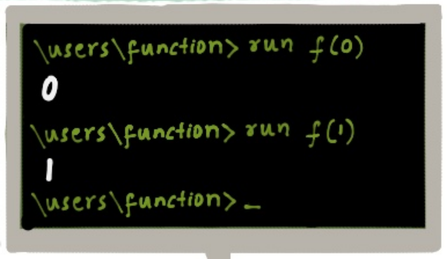
$f(x) = 1$

$f(x) = x$ > EQUALLY BALANCED OUTPUT

$f(x) = NOT(x)$

## THE FAMILIAR CLASSICAL APPROACH

$f(0) = 0$
$f(1) = 0$
$f(0) = 1$
$f(1) = 1$




RUN f() TWICE

$f(0) = 0$
$f(1) = 1$
$f(0) = 1$
$f(1) = 0$

## THE QUANTUM WAY



I am an Oracle

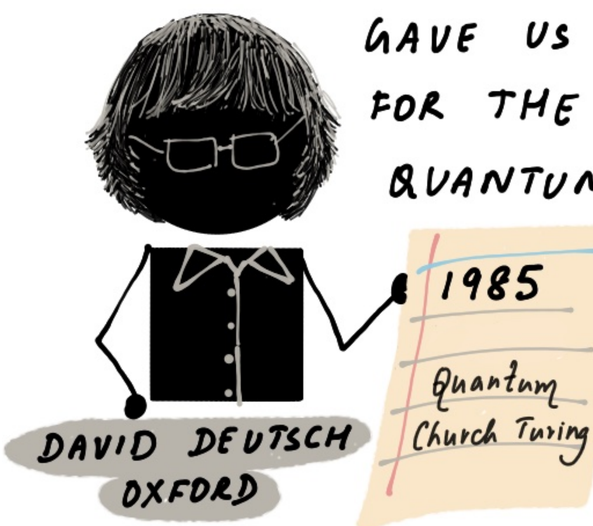
Am I Constant ?

Am I Balanced ?

You may ask me

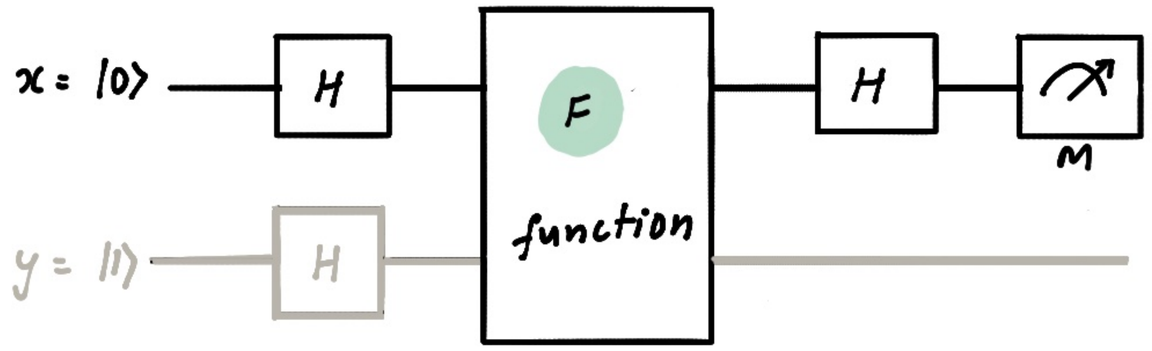
Just once

## DAVID DEUTSCH - 1990s




GAVE US THE TEMPLATE FOR THE VERY FIRST QUANTUM ALGORITHM WITH GOOD MATHEMATICAL ABSTRACTION

# DEUTSCH-JOZSA ALGORITHM: CORE




A QUANTUM CIRCUIT READS FROM LEFT TO RIGHT

INPUT QUBIT $x = 0$
HELPER QUBIT $y = 1$

→ GO THROUGH HADAMARD GATES → THAT SET THEM IN EQUAL SUPERPOSITION



AN ORACLE FUNCTION F RETURNS
0 → CONSTANT
1 → BALANCED

A SINGLE MEASUREMENT [↗] AT THE END REVEALS IF F IS CONSTANT / BALANCED

# IMPLEMENTING THE ORACLE

THERE ARE 4 OPTIONS $f(x)=0$, $f(x)=1$, $f(x)=x$, $f(x)=\text{NOT } x$

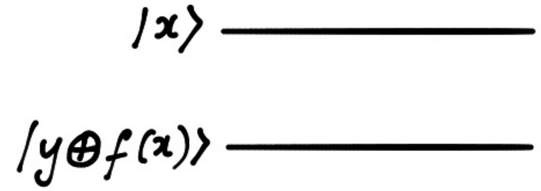
LET'S SAY THE FUNCTION OUTPUTS $|x\rangle$ AND $|y \oplus f(x)\rangle$ where $\oplus$ = XOR

CONSTANT

## CASE ① $f(x)=0$

| x | y | $y \oplus f(x)$ |
|---|---|---|
| 0 | 1 | 1 |
| 1 | 1 | 1 |
| 0 | 0 | 0 |
| 1 | 0 | 0 |

CIRCUIT



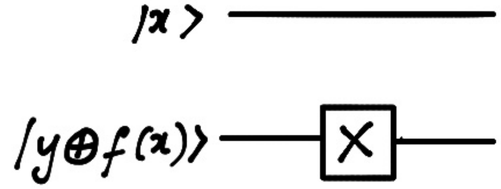

OUTPUT = $|x\rangle\,|y\rangle$

CONSTANT

## CASE ② $f(x)=1$

| x | y | $y \oplus f(x)$ |
|---|---|---|
| 0 | 1 | 0 |
| 1 | 1 | 0 |
| 0 | 0 | 1 |
| 1 | 0 | 1 |

CIRCUIT



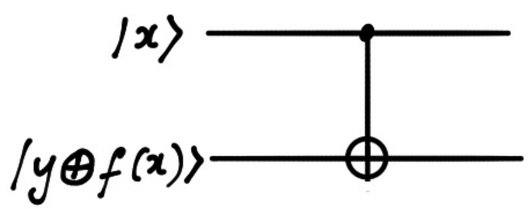

OUTPUT = $|x\rangle$ NOT $|y\rangle$

BALANCED

## CASE ③ $f(x)=x$

| x | y | $y \oplus f(x)$ |
|---|---|---|
| 0 | 1 | 1 |
| 1 | 1 | 0 |
| 0 | 0 | 0 |
| 1 | 0 | 1 |

CIRCUIT



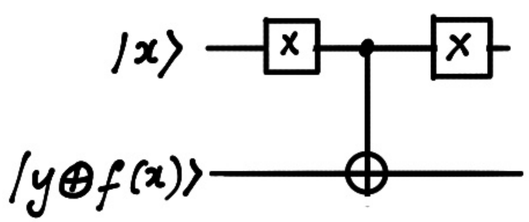

$y \oplus f(x)$ acts like CNOT

BALANCED

## CASE ④ $f(x)=\text{NOT } x$

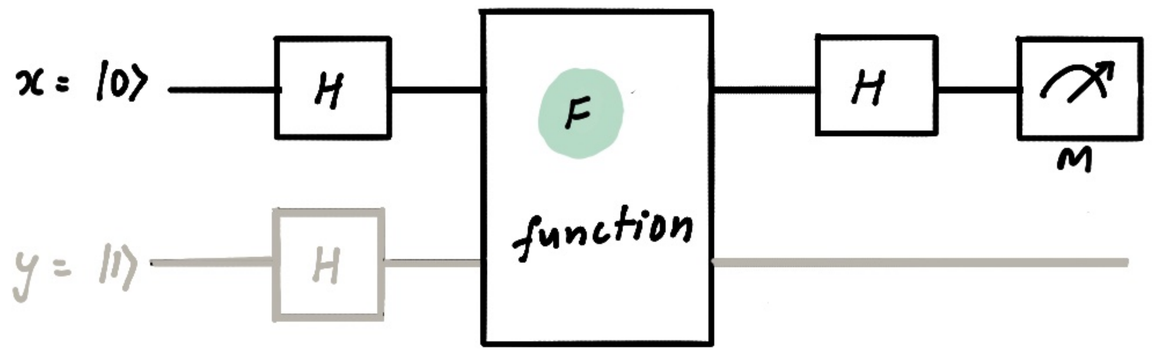
| x | y | $y \oplus f(x)$ |
|---|---|---|
| 0 | 1 | 0 |
| 1 | 1 | 1 |
| 0 | 0 | 1 |
| 1 | 0 | 0 |

CIRCUIT




$y \oplus f(x)$ is a "reverse" CNOT

# DEUTSCH-JOZSA: DETAIL - 1




AFTER 2 HADAMARD GATES

$$x, y \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$x, y \rightarrow \frac{1}{2}\left[|00\rangle + |11\rangle - |01\rangle - |11\rangle\right] \rightarrow \text{combined state of } x, y$$

WHEN THEY PASS THROUGH F, THE OUTPUT IS $x, y \oplus f(x)$

$$\frac{1}{2}\left[|0\ 0\oplus f(0)\rangle + |1\ 0\oplus f(1)\rangle - |0\ 1\oplus f(0)\rangle - |1\ 1\oplus f(1)\rangle\right]$$

# DEUTSCH-JOZSA: DETAIL - 2

$$\frac{1}{2}\left[|0\,0\oplus f(0)\rangle + |1\,0\oplus f(1)\rangle - |0\,1\oplus f(0)\rangle - |1\,1\oplus f(1)\rangle\right]$$

**CONSTANT $f(0) = f(1) = 0$**

- $|00\rangle + |10\rangle - |01\rangle - |11\rangle$

Pull out common terms

- $|0\rangle(|0\rangle - |1\rangle) + |1\rangle(|0\rangle - |1\rangle)$

2nd qubit

- $+(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$

**CONSTANT $f(0) = f(1) = 1$**

- $|01\rangle + |11\rangle - |00\rangle - |10\rangle$

Pull out common terms

- $|0\rangle(|1\rangle - |0\rangle) + |1\rangle(|1\rangle - |0\rangle)$

2nd qubit

- $-(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$

**BALANCED $f(0) = 0$ $f(1) = 1$**

- $|00\rangle + |11\rangle - |01\rangle - |10\rangle$

Pull out common terms

- $|0\rangle(|0\rangle - |1\rangle) + |1\rangle(|1\rangle - |0\rangle)$

2nd qubit

- $(-1)(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$

**BALANCED $f(0) = 1$ $f(1) = 0$**

- $|01\rangle + |10\rangle - |00\rangle - |11\rangle$

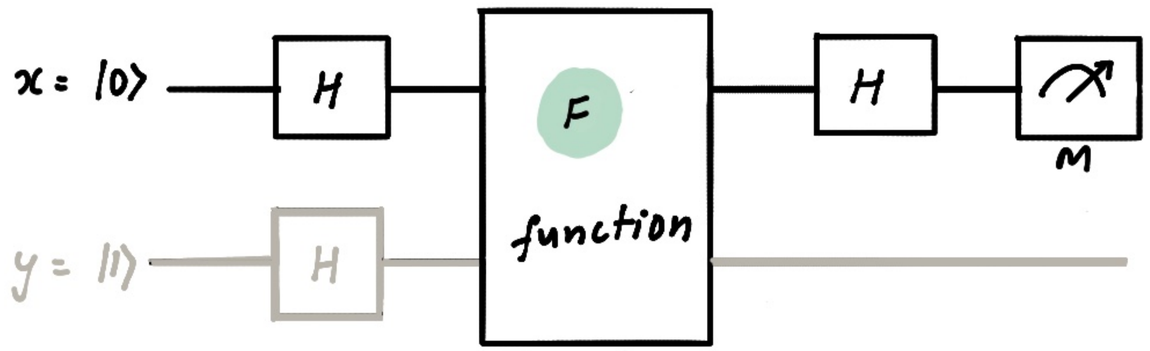
Pull out common terms

- $|0\rangle(|1\rangle - |0\rangle) + |1\rangle(|0\rangle - |1\rangle)$

2nd qubit

- $-(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$

# DEUTSCH-JOZSA: MEASURE




$$\frac{1}{2}\left[|0\,0\oplus f(0)\rangle + |1\,0\oplus f(1)\rangle - |0\,1\oplus f(0)\rangle - |1\,1\oplus f(1)\rangle\right]$$

BECOMES

**FOR CONSTANT FUNCTIONS**

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- QUBIT 1 IS IN STATE $|+\rangle$
- $H|+\rangle$ GIVES $|0\rangle$

**FOR BALANCED FUNCTIONS**

$$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes (\pm)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- QUBIT 1 IS IN STATE $|-\rangle$
- $H|-\rangle$ GIVES $|1\rangle$

MEASURE TO GET

0 → CONSTANT  1 → BALANCED

# DEUTSCH-JOZSA: ANOTHER VIEW

EFFECTIVELY, THE FIRST QUBIT IS MULTIPLIED BY $(-1)^{f(x)}$

## MEASUREMENT RETURNS 0

IF $f(0) = f(1)$ : **CONSTANT**

$$F|+\rangle = \frac{(-1)^{f(x)}}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$= \frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle$$

$$= |+\rangle$$

$$H|+\rangle = |0\rangle$$

## MEASUREMENT RETURNS 1

IF $f(0) \neq f(1)$ : **BALANCED**

$$F|+\rangle = \frac{(-1)^{f(x)}}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$= \frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle$$

$$= |-\rangle$$

$$H|-\rangle = |1\rangle$$

# GROVER'S ALGORITHM FOR UNSORTED SEARCH

# GROVER'S ALGORITHM

## THE PROBLEM: FIND THE NEEDLE




## THE FAMILIAR CLASSICAL APPROACH

LOOKING FOR A NEEDLE AMONG N UNORDERED ITEMS REQUIRES




- N/2 TRIES AT BEST
- N TRIES AT MOST

## GROVER'S ALGORITHM



LOV K GROVER
BELL LABS

1996
A fast quantum mechanical algorithm for database search

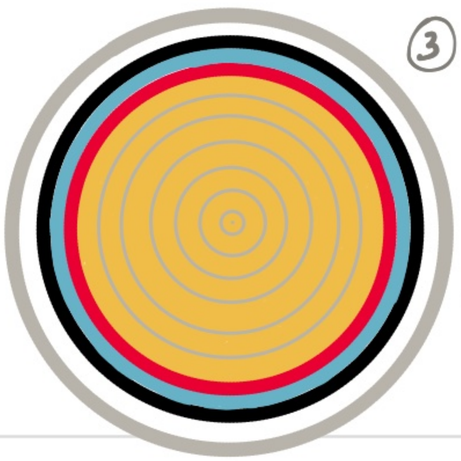
ACHIEVES QUANTUM SPEED UP FINDING 'NEEDLES' IN ONLY $\sqrt{N}$ TRIES

GOING THROUGH A MILLION THINGS ONLY 1000 TIMES!

## THE QUANTUM WAY

1. IDENTIFY  THE ANSWER

2. INCREASE ITS AMPLITUDE AND

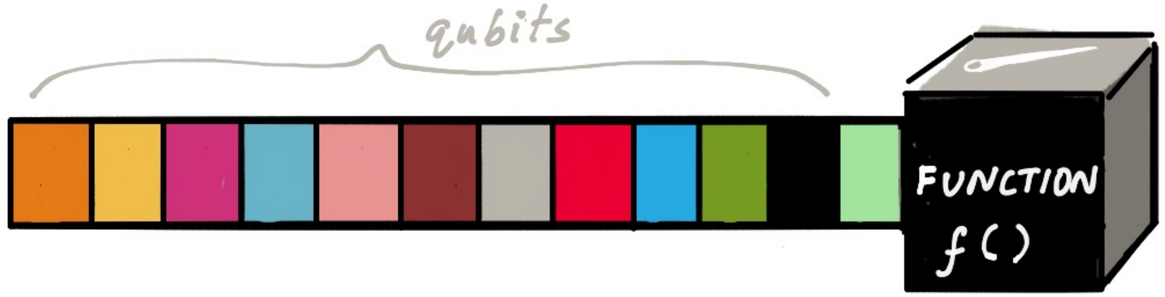


3. DECREASE ALL OTHER AMPLITUDES



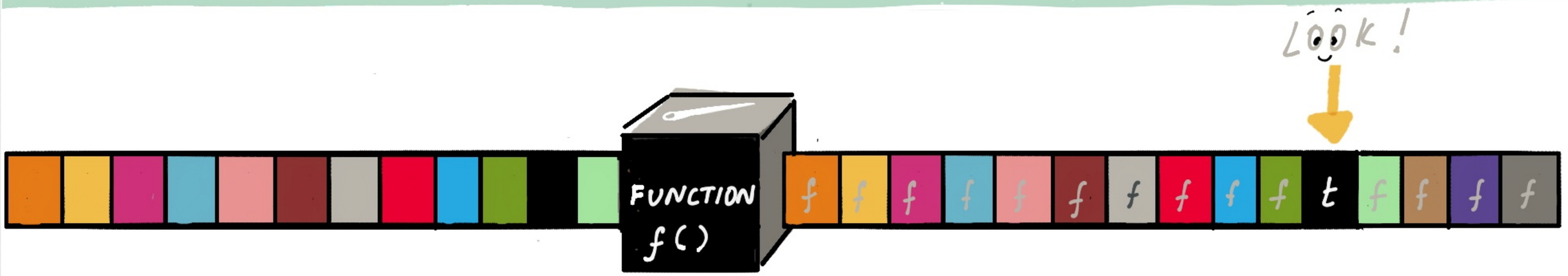
# GROVER-1 : INITIAL STEP

## INITIALISE




$n$ QUBITS IN EQUAL SUPERPOSITION REPRESENT $2^n = N$ ITEMS EACH WITH AMPLITUDE $1/\sqrt{N}$

## START THE SEARCH

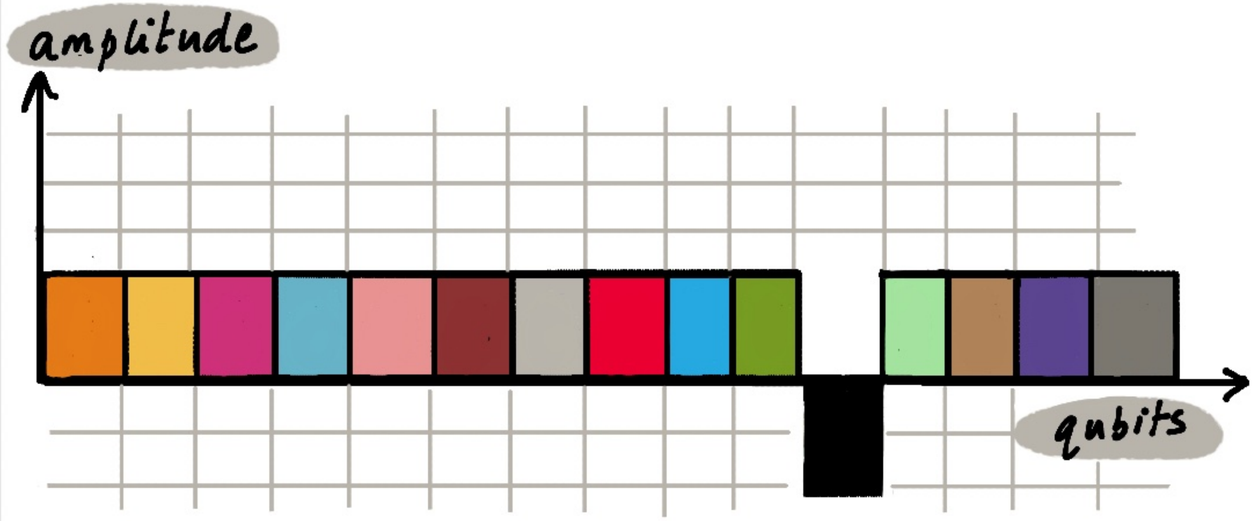



$f()$ QUERIES THE QUBITS AND IT RETURNS 1 - IF THE NEEDLE IS FOUND

0 - IF NOT FOUND

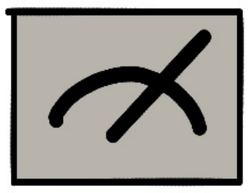
# GROVER – 2: INVERT PHASE

## INVERT THE PHASE




THE FUNCTION THEN FLIPS THE PHASE OF THE NEEDLE BY MULTIPLYING EACH QUBIT BY $(-1)^{f(x)}$

## MEASURE NOW?

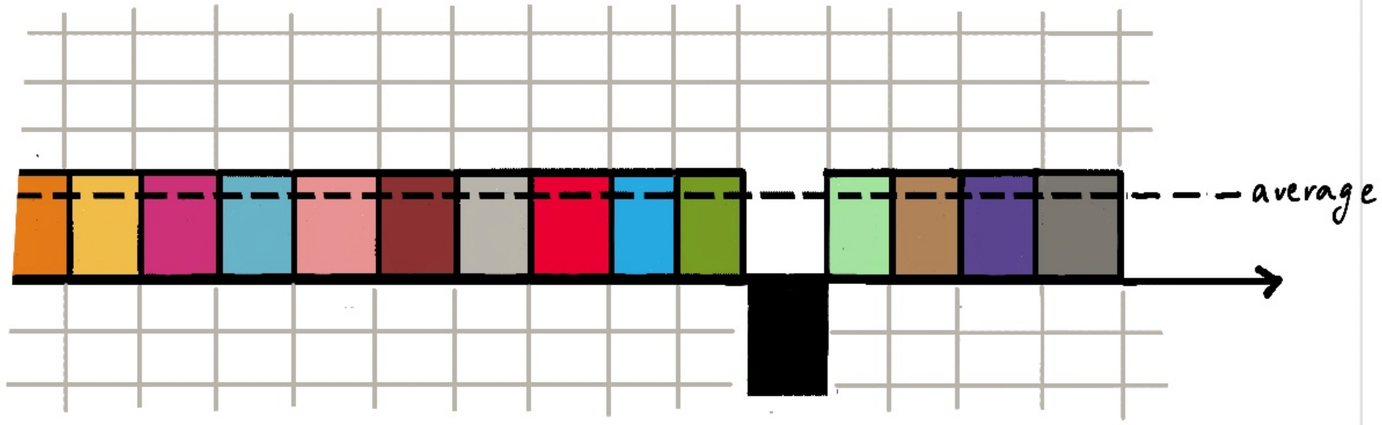


A MEASUREMENT WON'T HELP AT THIS STAGE, BECAUSE THE SUPERPOSITION WILL COLLAPSE TO A RANDOM STATE WITH A PROBABILITY $1/N$

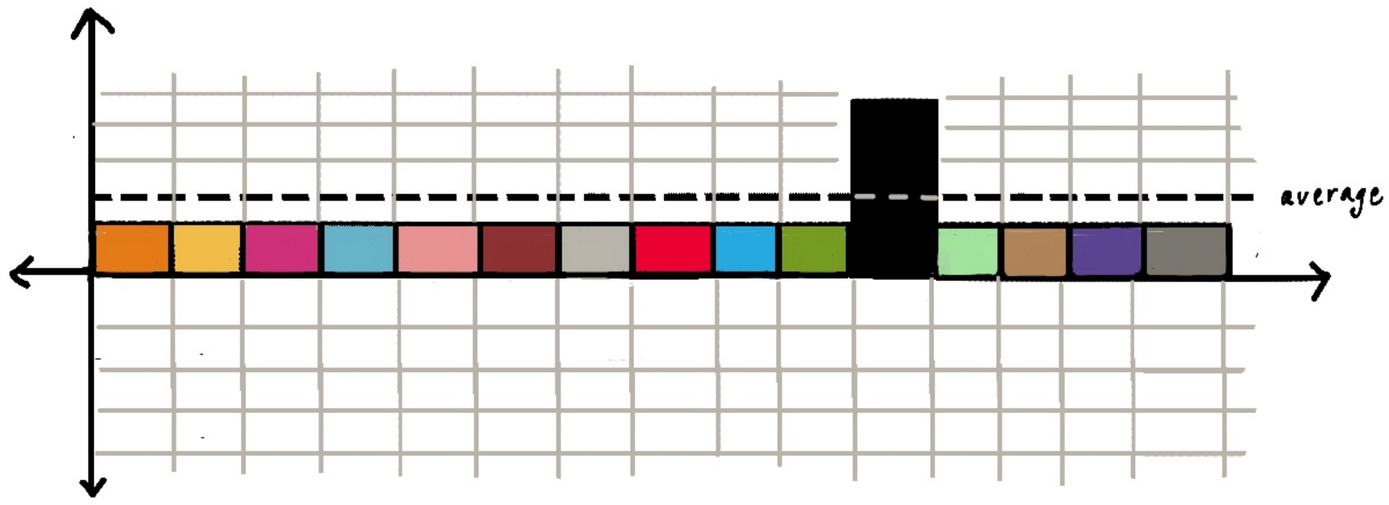
# GROVER – 3 : AMPLIFY ANSWER

## AMPLIFY THE ANSWER

FIND THE AVERAGE OF
ALL THE AMPLITUDES




THEN ROTATE
THE AMPLITUDES
ABOUT THE AVERAGE




THIS MEANS THAT THEY
ARE JUST AS FAR AWAY
FROM THE AVERAGE

BUT ON THE 'OTHER' SIDE

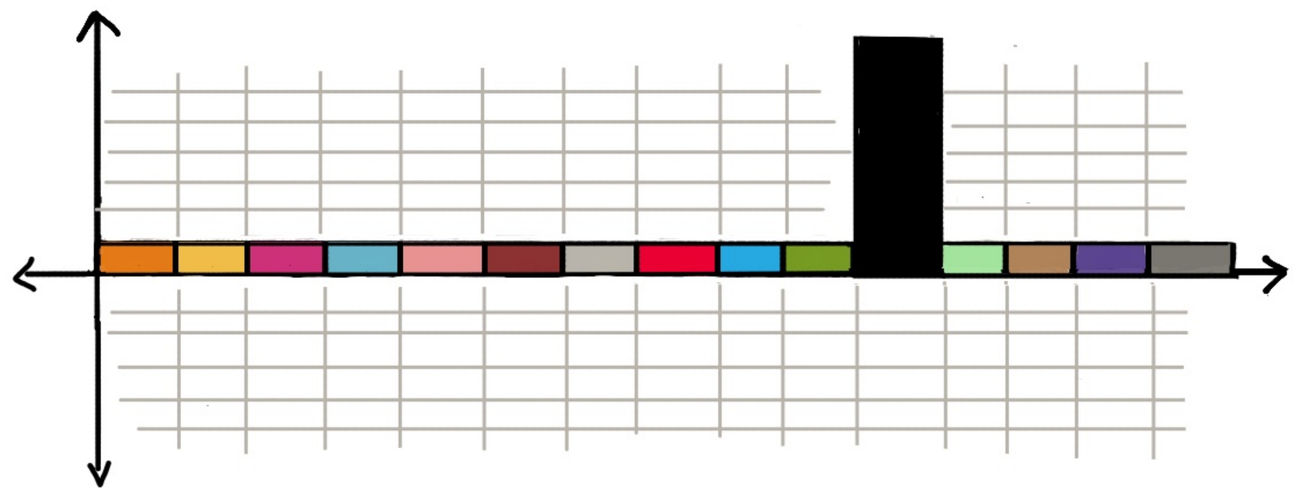
# GROVER - 4 : FIND NEEDLE

FIND THE NEEDLE

REPEAT ENOUGH TIMES

— ABOUT $\sqrt{N}$ TIMES —

UNTIL THE AMPLITUDE OF THE 'NEEDLE' IS HIGH



SO WHEN A MEASUREMENT IS MADE

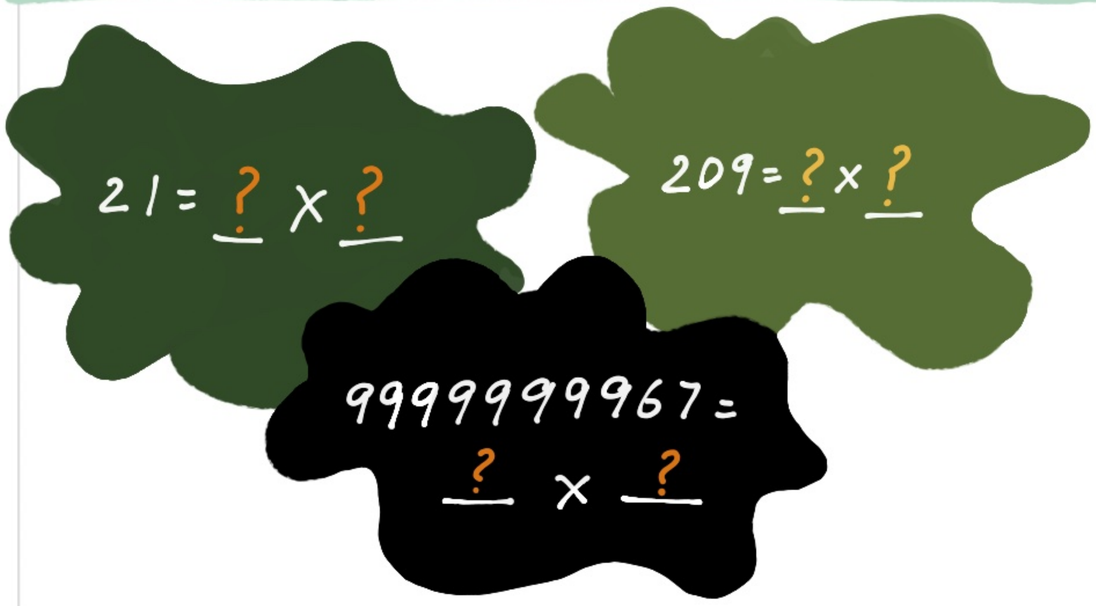
THE MOST LIKELY OUTCOME IS THE 'NEEDLE'

# SHOR'S ALGORITHM FOR FACTORING

— THE MOST FAMOUS QUANTUM ALGORITHM —

# SHOR'S ALGORITHM

## THE PROBLEM : FIND THE FACTORS



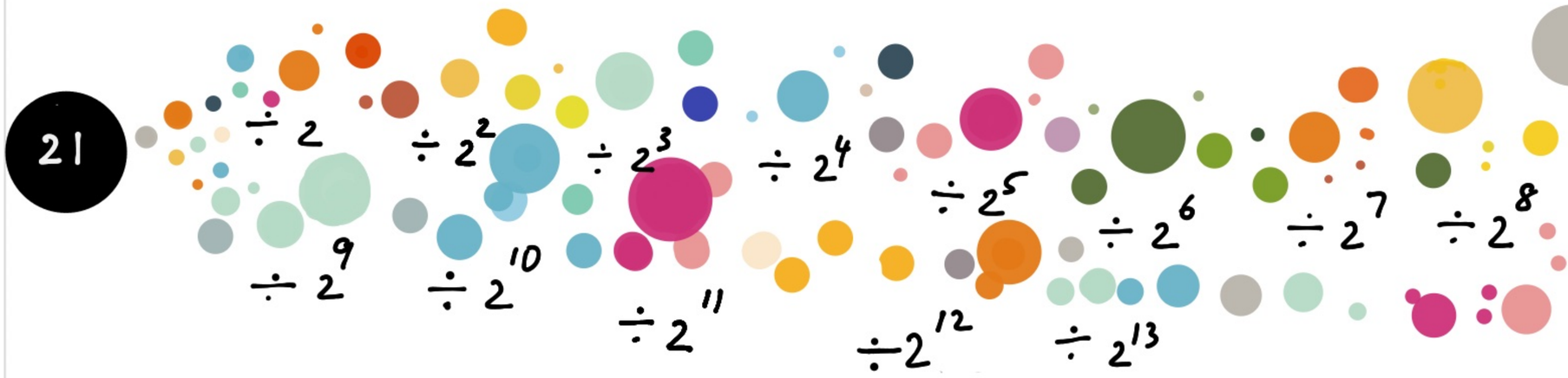

IN A REASONABLE AMOUNT OF TIME

## THE CLASSICAL APPROACH

```
for i = 2, i < √21, i++
    if 21 % i == 0
        return i
end for
```

TAKES EXPONENTIAL TIME
(even the special number field sieve)

## THE QUANTUM WAY - FINDS FACTORS IN POLYNOMIAL TIME






PETER SHOR
BELL LABS / MIT

# THE CORE OF SHOR'S ALGORITHM

SOLVE — find $x$

$x^2 = 1 \text{ MOD } N$

this means

TO FACTORISE $N$

$N \div x^2$ LEAVES REMAINDER 1

no remainder

$x^2 - 1$ DIVIDES $N$

perfectly

multiply it out

$x^2 - 1 = (x+1)(x-1)$

to check

IGNORE $x^2 = 1$

it's trivial

$N = 15$

$x^2 = 1 \text{ MOD } 15$

$16 = 1 \text{ MOD } 15$

$x^2 = 16$

$x = 4$

$16 - 1$ DIVIDES $N$

$(4+1)(4-1)$ DIVIDES $N$

$(5)(3)$ DIVIDES 15

FACTORS OF 15 ARE 5, 3

$N = 21$

$x^2 = 1 \text{ MOD } 21$

$64 = 1 \text{ MOD } 21$

$x^2 = 64$

$x = 8$

$64 - 1$ DIVIDES $N$

$(8+1)(8-1)$ DIVIDES $N$

$(9)(7)$ DIVIDES 21

FACTORS OF 21 ARE 3, 7

# HOW TO FIND X

**START WITH A GUESS**

Really?

**YES! PICK A RANDOM NUMBER**

$x = 2$

**RAISE IT TO EVERY POWER**

$2^1$ $2^2$ $2^3$ $2^4$...

**DIVIDE EACH BY N**

$\div 21$

**WRITE DOWN REMAINDERS**

2 4 8 16 ...

**FIND REMAINDER = 1**

$2^6 = 1 \text{ MOD } 21$

**LUCKY IF THE POWER IS EVEN**

so it has a square root!
That is, $x = 8$

**LOOK FOR REPEATING REMAINDERS**

I see repeating sets

| $N=21$ | $x=2$ | |
|---|---|---|
| | | MOD 21 |
| $2^1$ | 2 | 2 |
| $2^2$ | 4 | 4 |
| $2^3$ | 8 | 8 |
| $2^4$ | 16 | 16 |
| $2^5$ | 32 | 11 |
| $2^6$ | 64 | 1 |
| $2^7$ | 128 | 2 |
| $2^8$ | 256 | 4 |
| $2^9$ | 512 | 8 |
| $2^{10}$ | 1024 | 16 |

Looks like $x^2 = 1 \text{ MOD } N$

Looks like these numbers repeat

**HOW MANY IN A REPEATING SET?**

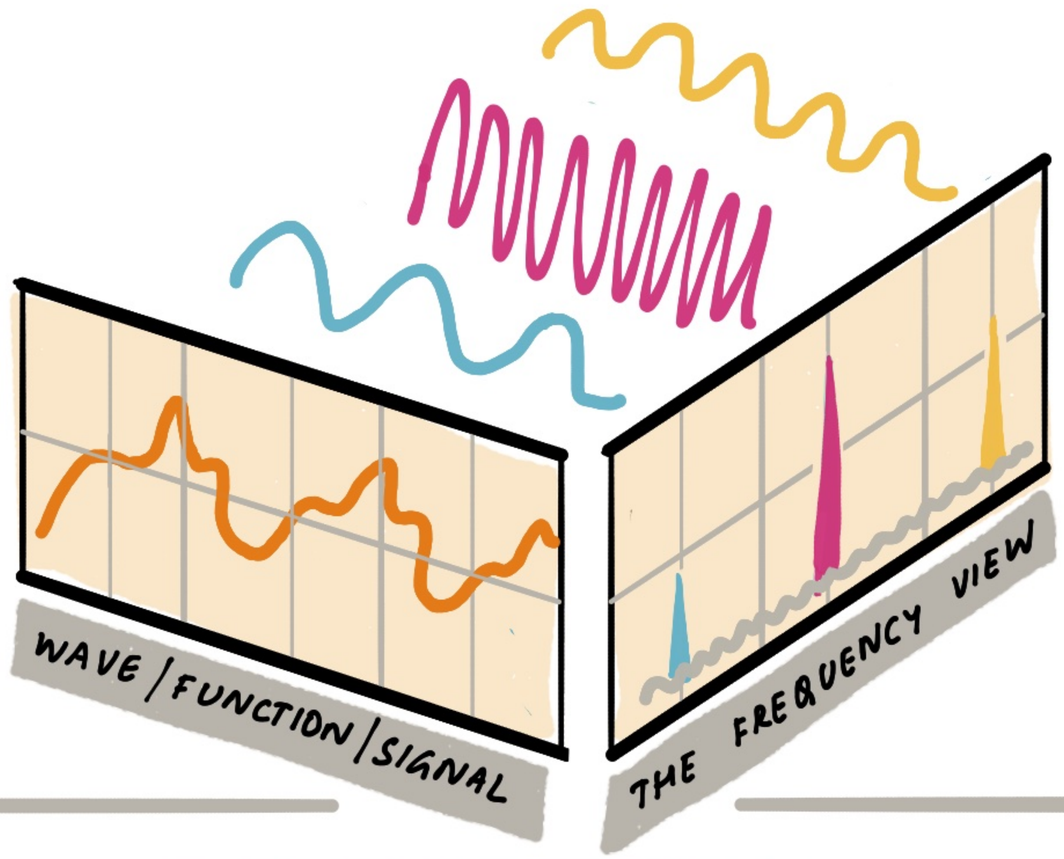
6 numbers

**SAME AS THE POWER OF THE GUESS IN THE $x^2 = 1 \text{ MOD } N$ ROW?**

Yes. No coincidence

**WELL, THAT'S THE PERIOD OF THE SEQUENCE**

# QUANTUM FOURIER TRANSFORM




A FOURIER TRANSFORM IS A MATHEMATICAL PROCESS APPLIED TO A WAVE / FUNCTION / SIGNAL

THIS IDENTIFIES THE INDIVIDUAL COMPONENTS & EACH FREQUENCY

THE PERIOD OF A WAVE IS THE INVERSE OF ITS FREQUENCY

## CONNECTION TO FACTORISATION

A QUANTUM VERSION OF THE FOURIER TRANSFORM IS APPLIED TO THE INPUT AND OUTPUT QUBITS IN SHOR'S ALGORITHM

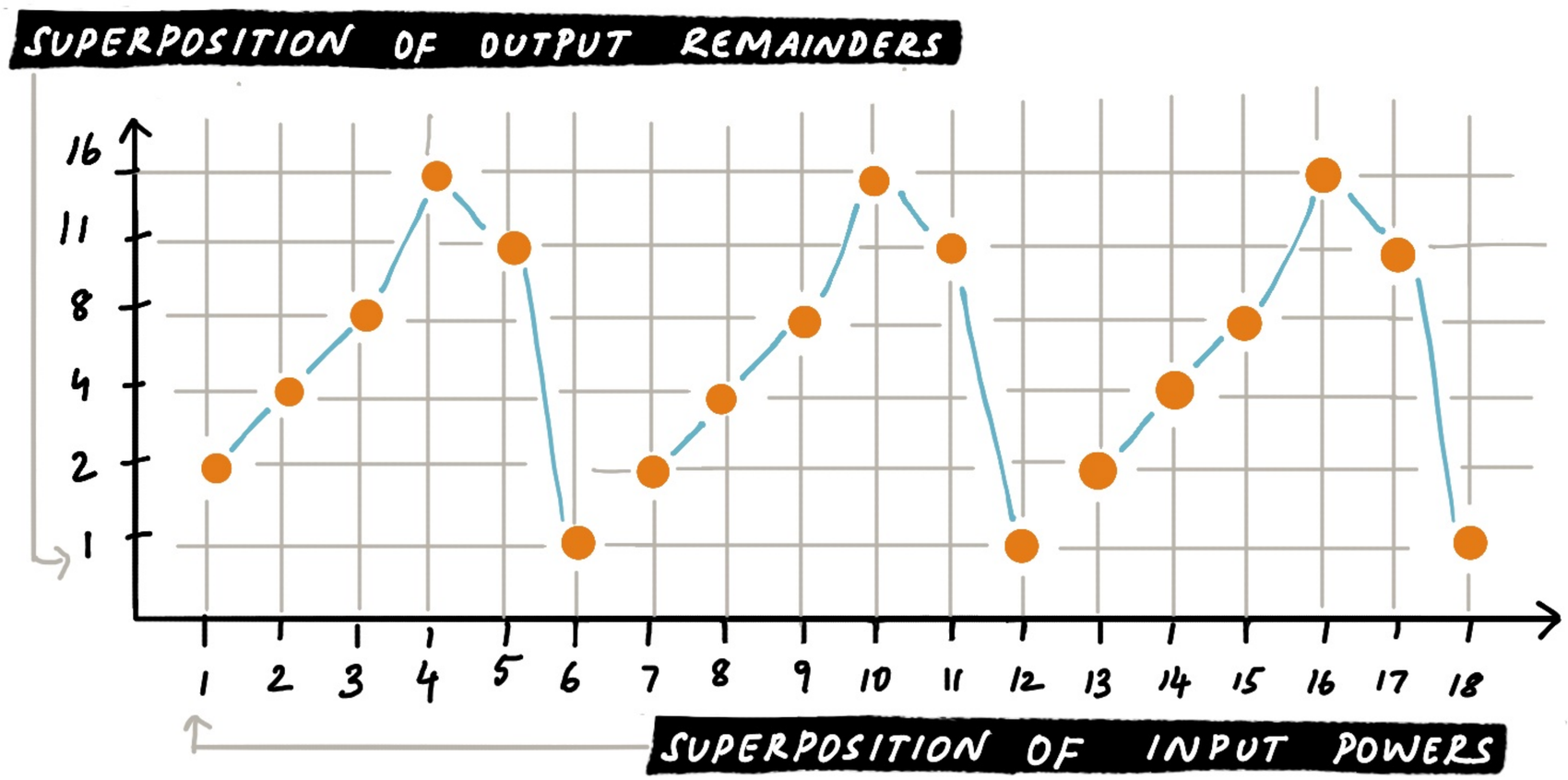
---

SO WHEN THE QUBITS ARE MEASURED/ SAMPLED FOR FREQUENCIES, WE CAN CALCULATE THE PERIOD WITH A GOOD PROBABILITY.

| CONTRIBUTORS | | | |
|---|---|---|---|
| JOSEPH | FOURIER | 1800s | original |
| CARL F. | GAUSS | 1800s | speed up |
| JOHN | COOLEY | 1960s | fast fourier transform |
| JOHN | TUKEY | | |
| DON | COPPERSMITH | 1990s-2000s | quantum fourier transform |

# PERIOD FINDING : STEP - 1

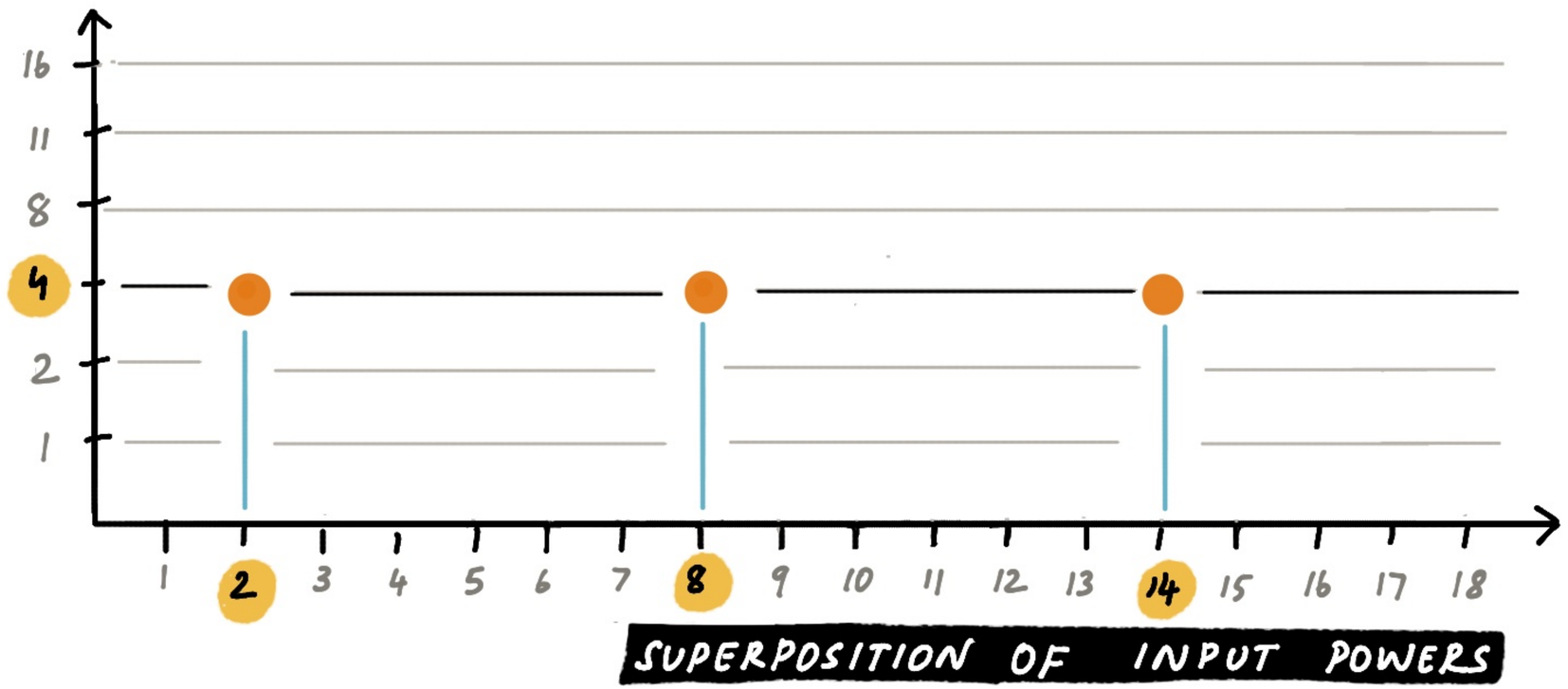
| Powers | Mod 21 |
|---|---|
| $2^1$ | 2 |
| $2^2$ | 4 |
| $2^3$ | 8 |
| $2^4$ | 16 |
| $2^5$ | 11 |
| $2^6$ | 1 |
| $2^7$ | 2 |
| $2^8$ | 4 |
| $2^9$ | 8 |
| $2^{10}$ | 16 |
| $2^{11}$ | 11 |
| $2^{12}$ | 1 |
| $2^{13}$ | 2 |
| $2^{14}$ | 4 |
| $2^{15}$ | 8 |
| $2^{16}$ | 16 |
| $2^{17}$ | 11 |
| $2^{18}$ | 1 |




- THE INPUT AND OUTPUT REGISTERS ARE ENTANGLED
- MEASURE THE OUTPUT REGISTER
- IT COLLAPSES TO A RANDOM VALUE - SAY 4

# PERIOD FINDING : STEP-2

| Powers | Mod 21 |
|---|---|
| $2^1$ | 2 |
| $2^2$ | 4 |
| $2^3$ | 8 |
| $2^4$ | 16 |
| $2^5$ | 11 |
| $2^6$ | 1 |
| $2^7$ | 2 |
| $2^8$ | 4 |
| $2^9$ | 8 |
| $2^{10}$ | 16 |
| $2^{11}$ | 11 |
| $2^{12}$ | 1 |
| $2^{13}$ | 2 |
| $2^{14}$ | 4 |
| $2^{15}$ | 8 |
| $2^{16}$ | 16 |
| $2^{17}$ | 11 |
| $2^{18}$ | 1 |




SUPERPOSITION OF INPUT POWERS

- THE INPUT REGISTER HAS ALSO NOW COLLAPSED TO ALL POWERS THAT LEAVE A REMAINDER 4
- THE PATTERN IS NOW:

  $x, x+p, x+2p \ldots\ldots$

  WHERE $p$ = PERIOD OF THE FUNCTION
- IDEALLY, WE WANT IT TO BE OF THE FORM

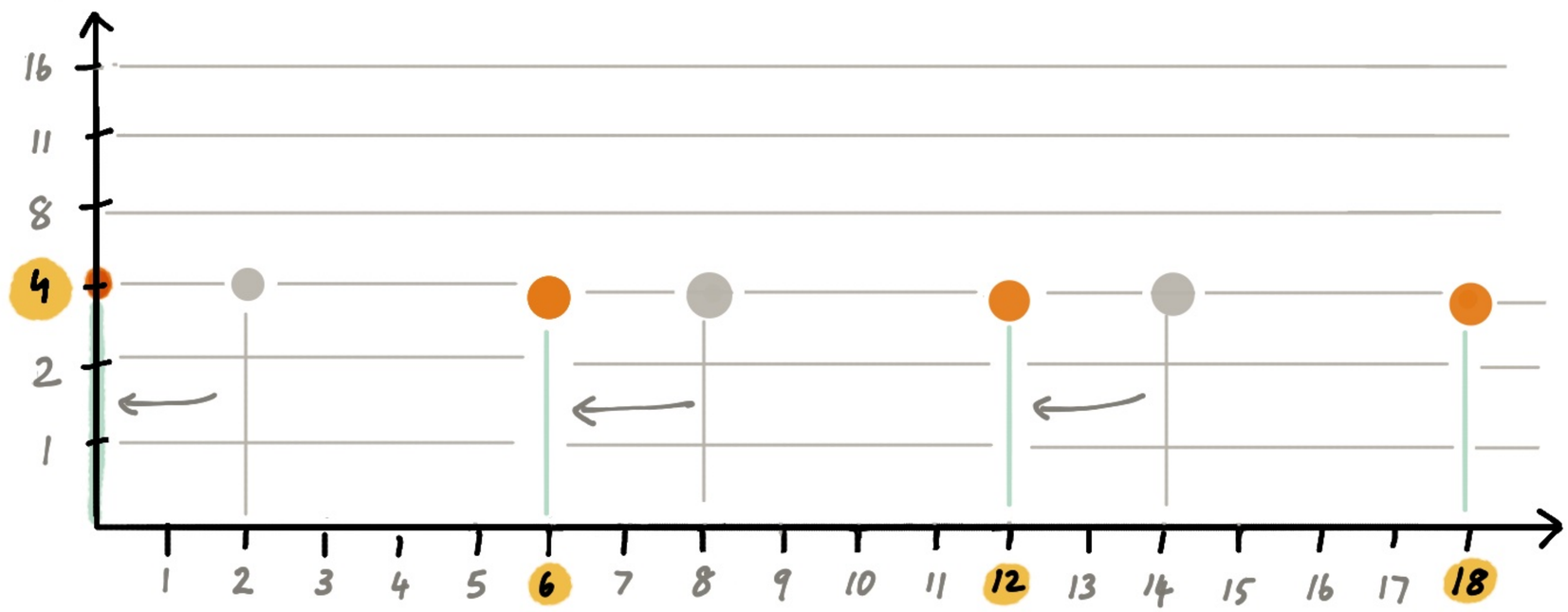
  $p, 2p, 3p, \ldots\ldots$

# PERIOD FINDING & FACTORING

SHIFT THE FIRST NON-ZERO VALUE TO ZERO

ALTERS:
- THE PHASE

DOES NOT ALTER:
- OUTPUT
- PERIOD




SHIFTED SUPERPOSITION OF INPUT POWERS

- MAKE MULTIPLE MEASUREMENTS : 12, 18, ...
- TAKE THE GREATEST COMMON DIVISOR OF THESE TO GET THE PERIOD = 6
- CHECK CLASSICALLY* WHETHER $(2^{6/2}-1)(2^{6/2}+1)$ DIVIDES $N = 21$
- $2^{6/2}-1$ IS 7 AND $2^{6/2}+1 = 9$. BOTH SHARE FACTORS WITH 21.
- IF NOT, CHANGE VALUES AND TRY AGAIN!

*An instance of quantum/classical computers working together

SO, QUANTUM COMPUTERS CAN SOLVE EVERYTHING?

# THOSE PROBLEMS - SOLVABLE?

NP-COMPLETE PROBLEMS (THE MAXIMALLY HARD PROBLEMS IN THE CLASS NP) ARE BELIEVED TO BE HARD TO SOLVE. HOWEVER, GIVEN A SOLUTION, IT IS EASY TO CHECK THAT IT IS CORRECT. SOME EXAMPLES BELOW:

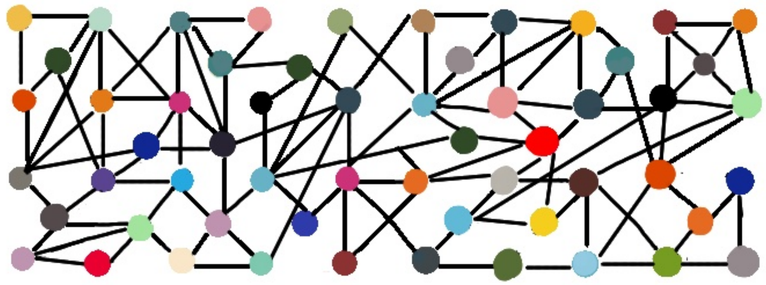
**SATISFIABILITY PROBLEM**

$(a = 1 \text{ OR } b = 0 \text{ OR } c = 1) \text{ AND}$

$(b = 1 \text{ OR } c = 0 \text{ OR } d = 1) \text{ AND}$

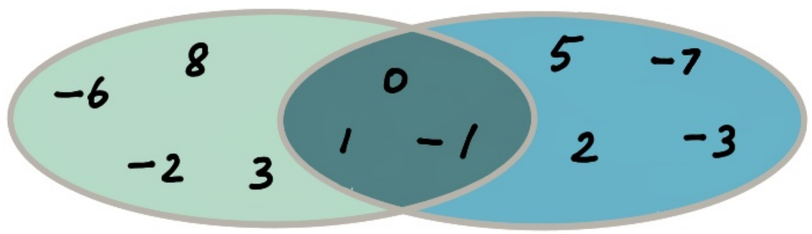
$(c = 1 \text{ OR } d = 0 \text{ OR } e = 1) \text{ AND} \ldots$

IS THERE A SOLUTION TO SATISFY THIS BOOLEAN FORMULA?



**CLIQUE PROBLEM**

IN MY SOCIAL NETWORK CAN I FIND THE LARGEST LIST OF PEOPLE WHO ALL KNOW EACH OTHER?




**SUBSET SUM PROBLEM**

IS THERE A (NON EMPTY) SUBSET WITH SUM = 0?

COULD ALL THE PERMUTATIONS/COMBINATIONS/OPTIONS BE SETUP INTO ONE MIGHTY SUPERPOSITION FOR A QUANTUM COMPUTER TO CHECK?

# WHAT A QUANTUM COMPUTER CANNOT DO



IT FEELS EASY TO THINK OF THE POWER OF A QUANTUM COMPUTER AS A GAZILLION PARALLEL COMPUTERS EXPLORING ALL POSSIBILITIES AT ONCE TO FIND THE CORRECT ANSWER EXPONENTIALLY FASTER. IN TRUTH:

CHECKING ALL POSSIBLE "PARALLEL" STATES IS NOT POSSIBLE IN A QUANTUM COMPUTER

A QUANTUM COMPUTER ALSO NEEDS A FEW TRIES BEFORE IT ARRIVES AT AN ANSWER

NOT ALL PROBLEMS CAN BE SPEEDED UP WITH QUANTUM COMPUTERS

# QUANTUM ALGORITHM EFFICIENCY



QUANTUM PARALLELISM

CHOOSING THE RIGHT PROBLEM

EFFICIENCY COMES FROM

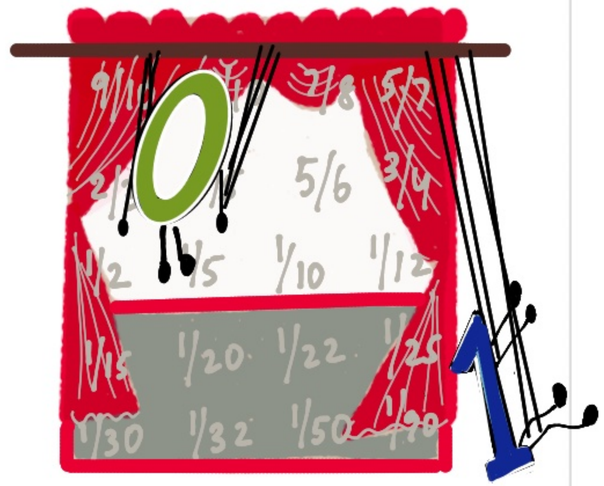
MANIPULATING PROBABILITIES



SUPERPOSITION

ENTANGLEMENT



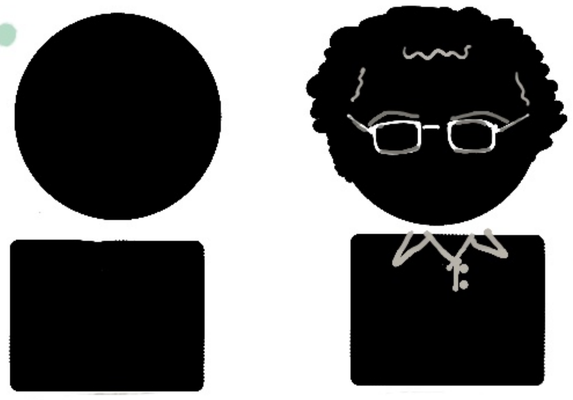


# BQP - A NEW COMPLEXITY CLASS

A NEW COMPLEXITY CLASS FOR A QUANTUM WORLD

BOUNDED ERROR QUANTUM POLYNOMIAL TIME

DEFINED BQP IN 1993



LAID FOUNDATIONS OF QUANTUM COMPLEXITY

ETHAN BERNSTEIN

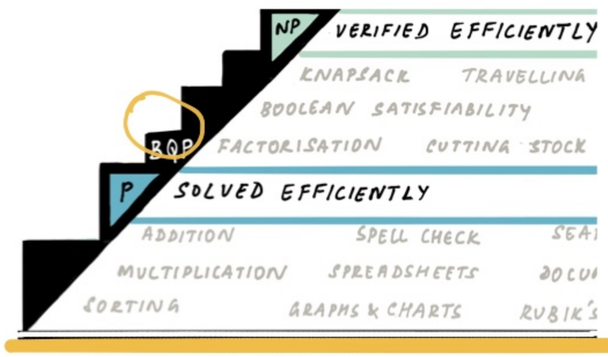
UMESH VAZIRANI

PROBLEMS : YES/NO DECISION

SOLVED BY : QUANTUM COMPUTERS

TIME : POLYNOMIAL

ERRORS : WITHIN A CERTAIN LIMIT




BQP CONTAINS P

BUT WHAT WE DON'T YET KNOW:

- IS NP CONTAINED IN BQP?
- CAN WE SOLVE EVEN MORE PROBLEMS?

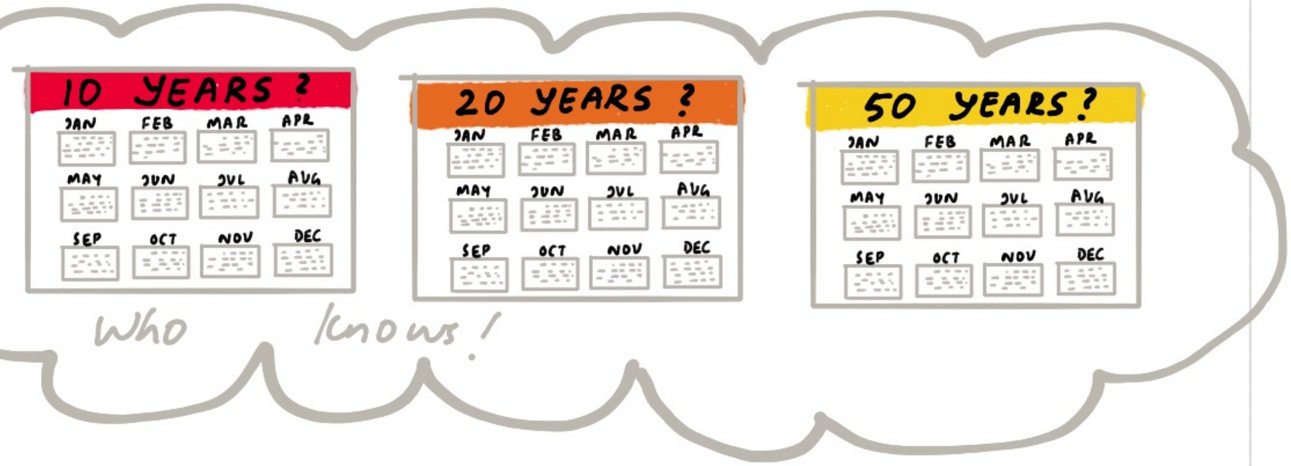
# SECURITY IN THE TIME OF QUANTUM

# QUANTUM CAN BREAK CRYPTO

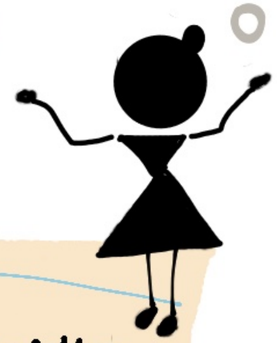
— 2019 —
Quantum Physics
How to factor 2048 RSA integers in 8 hours using 2 million noisy qubits
Craig Gidney, Martin Ekera



IT SEEMS ONLY A MATTER OF TIME THAT QUANTUM COMPUTERS WILL BREAK ALL ENCRYPTION SYSTEMS THAT HOLD OUR ONLINE INFORMATION SECURE




2019 : THE TOP PROGRAMMABLE QUANTUM COMPUTER HAS 53 QUBITS



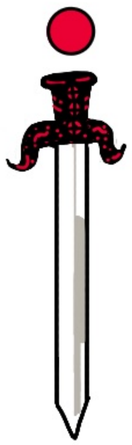
— 2015 —
Quantum Physics
Applying Grover's Algorithm to AES : quantum resource estimates
Grassi, Langenberg, Roetteler, Steinwandt

ONLINE SECURITY : THINGS TO LOOK OUT FOR

- QUANTUM-SAFE CRYPTOSYSTEMS
- ENOUGH ERROR-CORRECTED QUBITS

# QUANTUM-SAFE CRYPTO

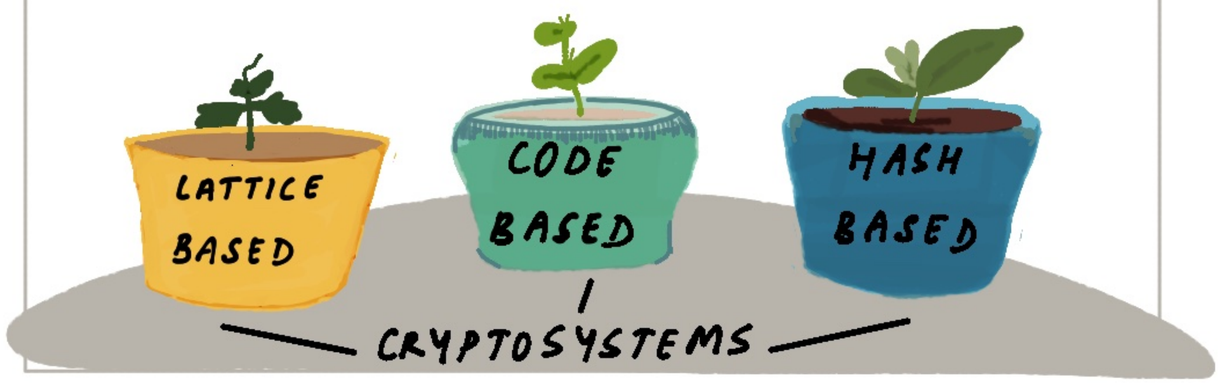
## CURRENT CRYPTO UNDER THREAT



- RSA
- DIFFIE-HELLMAN
- ELLIPTIC CURVE
- DIGITAL SIGNATURES AND SECURITY PROTOCOLS/PRODUCTS BASED ON THEM

## NEW RESEARCH

- FOR A POST-QUANTUM WORLD



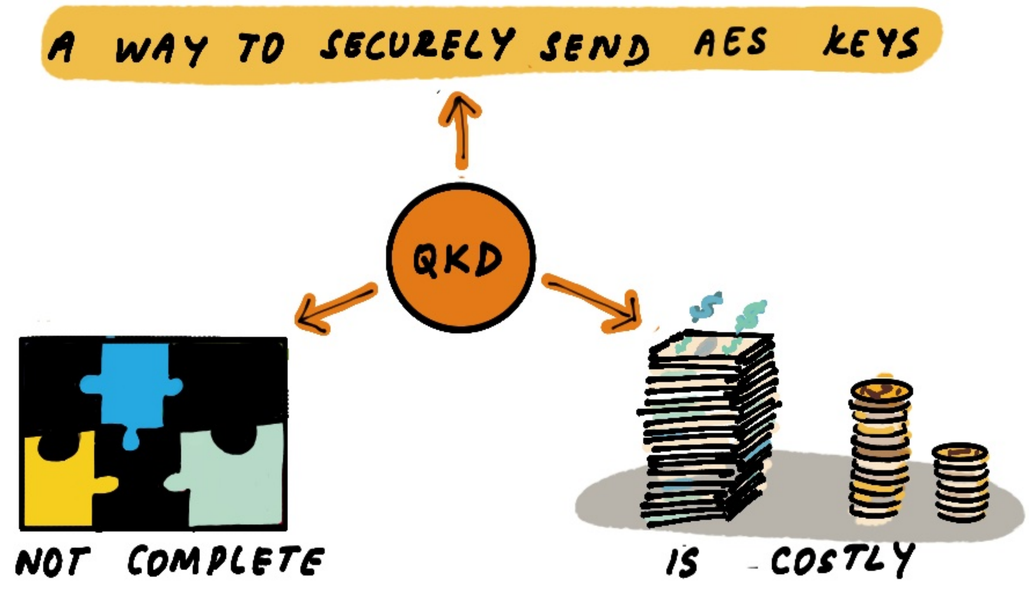

## KNOWN QUANTUM-SAFE CRYPTO



- SOME SYMMETRIC KEY CRYPTO
  - ONE-TIME PAD
  - AES
- SOME HASH FUNCTIONS

REFER: ETSI.DRG QUANTUM SAFE WHITEPAPER

## QUANTUM KEY DISTRIBUTION - QKD

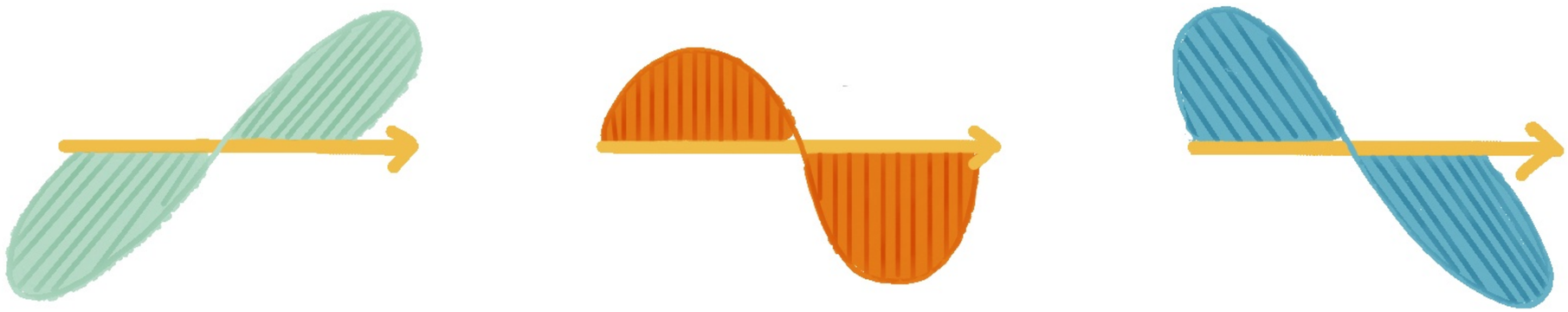



REFER: NCSC.GOV.UK QKD WHITEPAPER

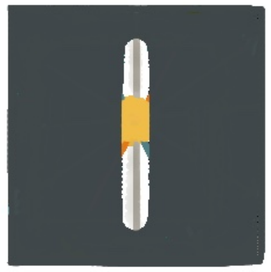
# QKD & POLARISATION

QUANTUM KEY DISTRIBUTION WORKS WITH POLARISED LIGHT

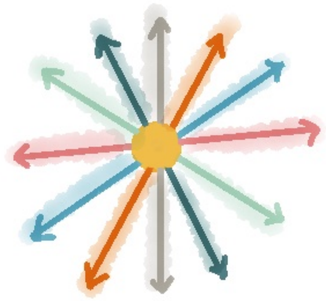
— HERE IS A BRIEF NOTE ON POLARISATION —



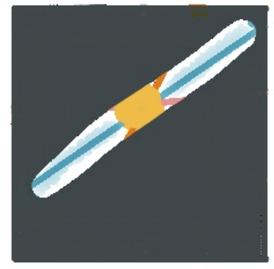
PHOTONS VIBRATE ON PLANES PERPENDICULAR TO THE DIRECTION OF LIGHT



RECTILINEAR FILTER



UNPOLARISED LIGHT



DIAGONAL FILTER

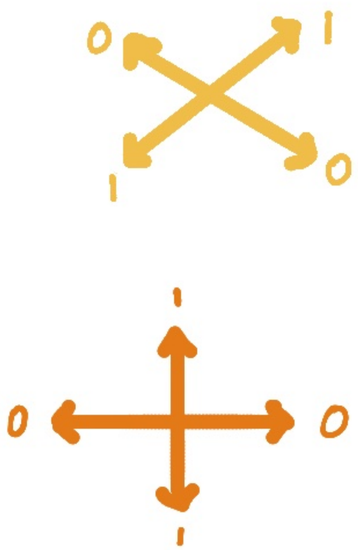
A POLARISING FILTER (LIKE SUNGLASSES) CHOOSES A PLANE

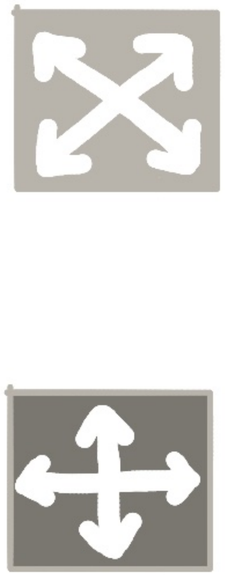
LETTING ONLY THOSE PHOTONS PASS THROUGH - MAKING POLARISED LIGHT

# QUANTUM KEY DISTRIBUTION - QKD

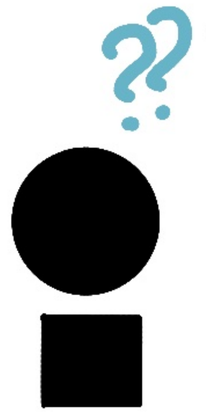



ALICE SENDS POLARISED LIGHT WHICH ENCODES BITS RANDOMLY IN ONE OF 2 METHODS



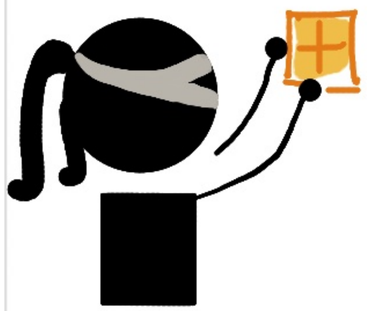



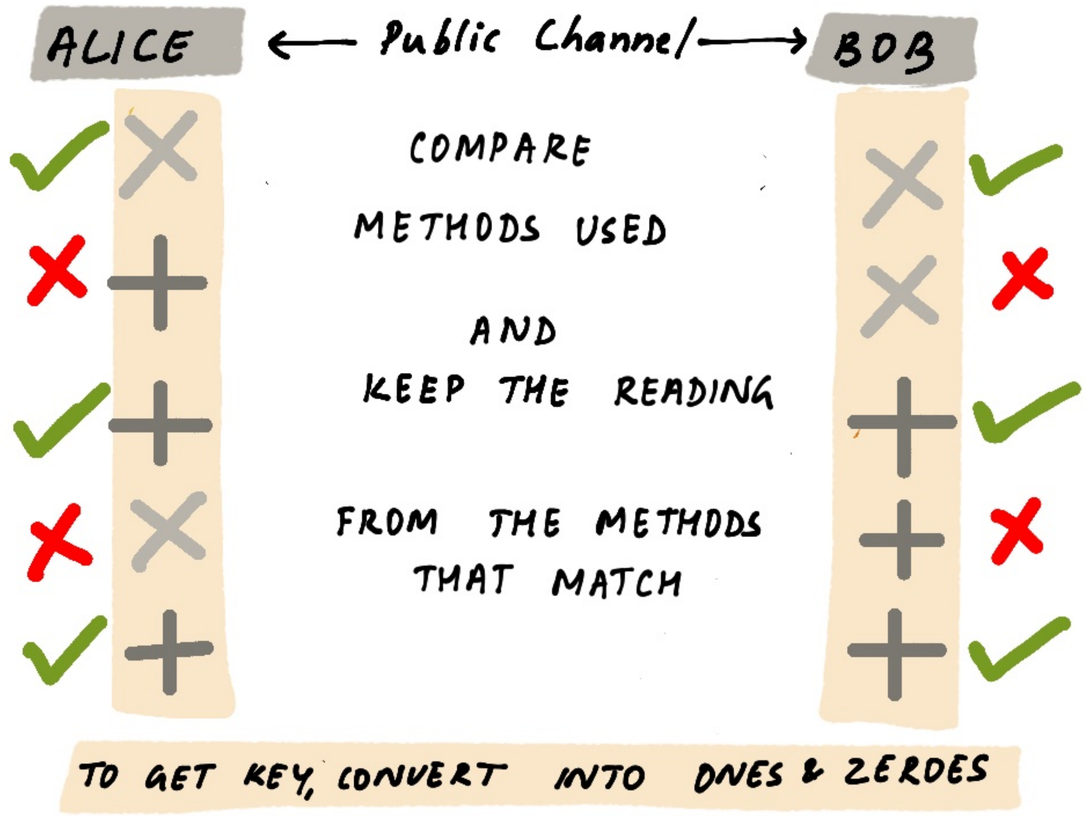
BOB MUST GUESS WHICH METHOD AND 'READ' THE PHOTON



AN EAVESDROPPER WILL END UP CHANGING THE POLARISATION

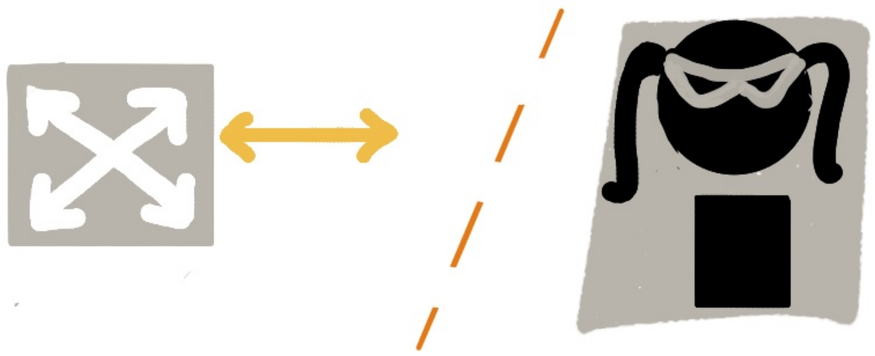






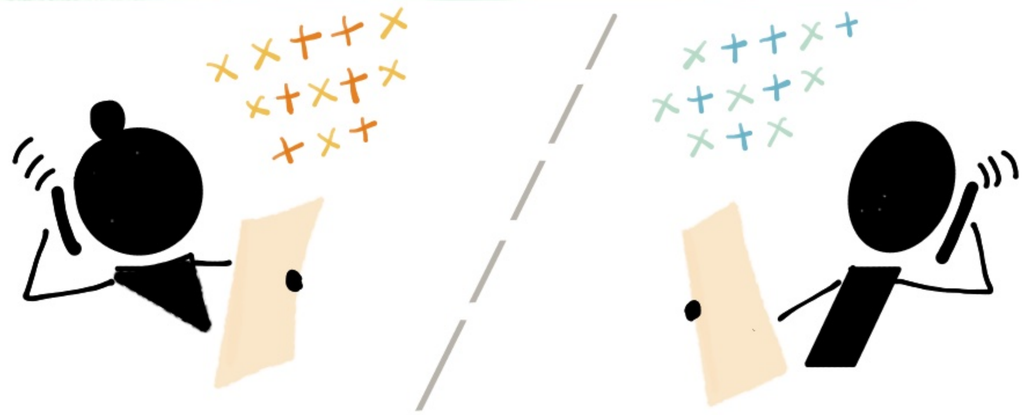
# GETTING THE SECRET KEY WITH QKD

## WRONG FILTER OR AN EAVESDROPPER



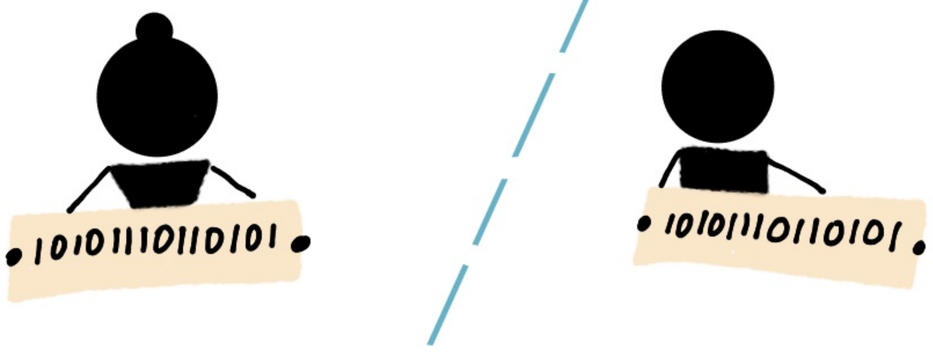
CAUSE ERRORS IN THE READING AND CAN BE IDENTIFIED

## IDENTIFY DISCREPANCIES



ONLY COMPARE THE FILTERS (NOT BITS) OVER A PUBLIC CHANNEL

## USE MATCHING READINGS




TRANSLATE THEM PRIVATELY

TO GET IDENTICAL STRINGS OF 0s AND 1s

## HAS EVE BEEN EAVESDROPPING?

= Compare a subset of the strings

● IF THEY MATCH : # No Eve

Use the other subset as key

● IF THEY DON'T MATCH : #Eve

Start over

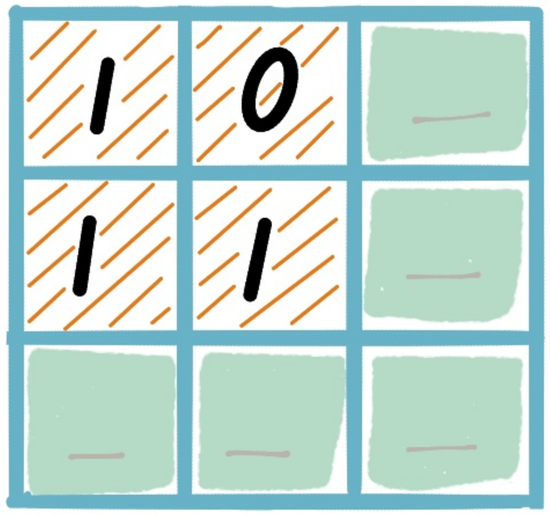
BASED ON THE BB84 PROTOCOL BY BENNETT AND BRASSARD

# ERROR CORRECTION

— TO MAKE QUBIT OPERATIONS MORE ACCURATE —

# CLASSICAL ERROR CORRECTION

ORIGINAL DATA



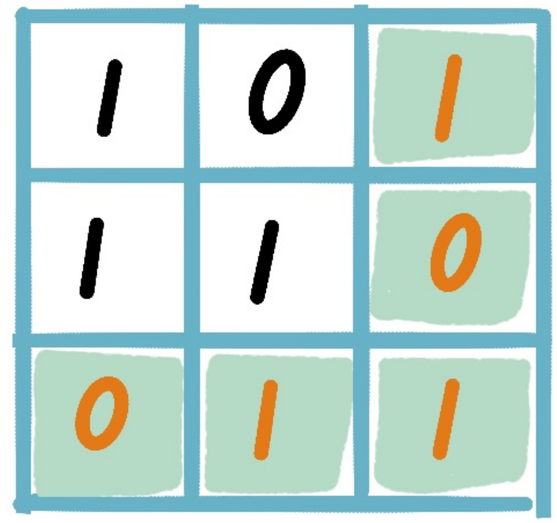

– SPACE FOR ERROR CORRECTION CODES

HOW MANY ONES PER ROW / COLUMN?

0 – IF EVEN

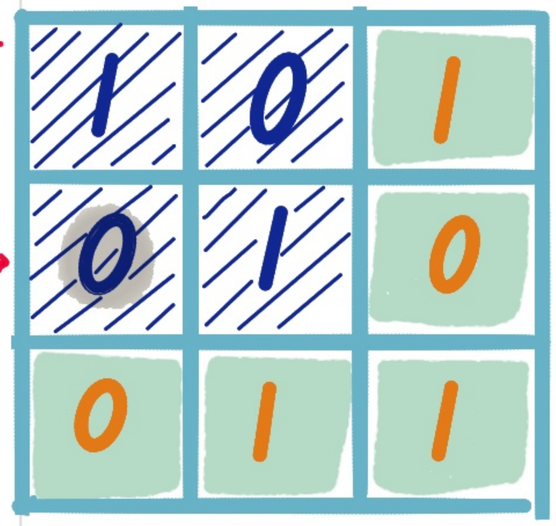
1 – IF ODD

ERROR CORRECTION APPLIED




corrupted data

IF THERE ARE DATA ERRORS




DOES THE DATA AGREE WITH THE ERROR CORRECTION CODES?

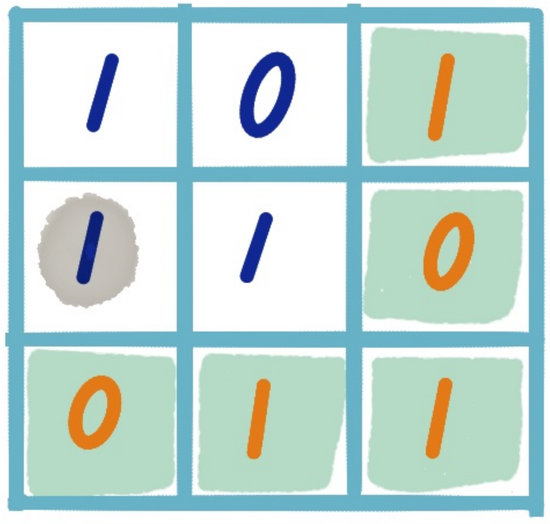
ROW 1 – ✓

ROW 2 – ✗

COL 1 – ✗

COL 2 – ✓

ERRORS CAN BE SPOTTED AND FIXED




THIS TYPE OF ERROR CORRECTION IS INTEGRAL TO HARDWARE DESIGN

THAT WE NOW TAKE FOR GRANTED

# QUANTUM ERROR CORRECTION (QEC)

## QUBITS ARE PRONE TO ERRORS

- DURING COMPUTATION
- FROM DECOHERENCE

## METHODS THAT WON'T WORK

- CHECKING VALUES
- BACKUPS

## BECAUSE...

- MEASUREMENT LOSES SUPERPOSITION
- 'NO-CLONING' THEOREM

## SOLUTION | APPROACH

MAKE A LOGICAL QUBIT

- SPREAD DATA ACROSS ENTANGLED QUBITS
- ADD ANCILLA (HELPER) QUBITS
- DETECT & CORRECT ERRORS BY READING THE ANCILLA QUBITS



PETER SHOR
BELL LABS/MIT

PETER SHOR CAME UP WITH THE FIRST THEORY OF QUANTUM ERROR CORRECTION USING 9 QUBITS TO ERROR CORRECT 1 QUBIT OF DATA

– 1995



JOHN PRESKILL
CALTECH

"WE ARE IN A **NISQ** NOISY INTERMEDIATE SCALE QUANTUM ERA (50-100 QUBIT COMPUTERS) A STEP TOWARD MORE POWERFUL QUANTUM TECHNOLOGIES OF THE FUTURE"

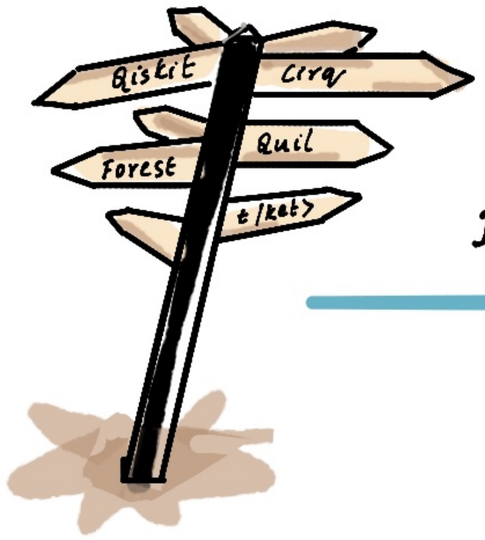
– 2017

# PROGRAMMING & TESTING

— THIS IS ANOTHER AREA OF ONGOING RESEARCH —

# PROGRAMMING

IT IS A CLASSICAL COMPUTER THAT ISSUES COMMANDS TO A QUANTUM COMPUTER TO EXECUTE VARIOUS GATES. OBVIOUSCY, THIS IS LOW LEVEL INSTRUCTION.




ALSO, MOST INSTRUCTION SETS OFFERED BY VARIOUS DEVELOPMENT KITS IN THE MARKET ARE TIED TO THE DEVICE.

WHAT DOES IT TAKE TO MAKE A HIGH LEVEL QUANTUM PROGRAMMING LANGUAGE?

— HERE ARE SOME OF THE CONSIDERATIONS —

- INSTRUCTIONS ARE HARDWARE INDEPENDENT & COMPILE
- OPENSOURCED FOR A COMMUNITY TO DEVELOP
- GOOD NUMBER OF ABSTRACT FUNCTIONS

  e.g ROUTINES FOR ERROR CORRECTION

  MEASUREMENTS, FOURIER TRANSFORMS

# TESTING

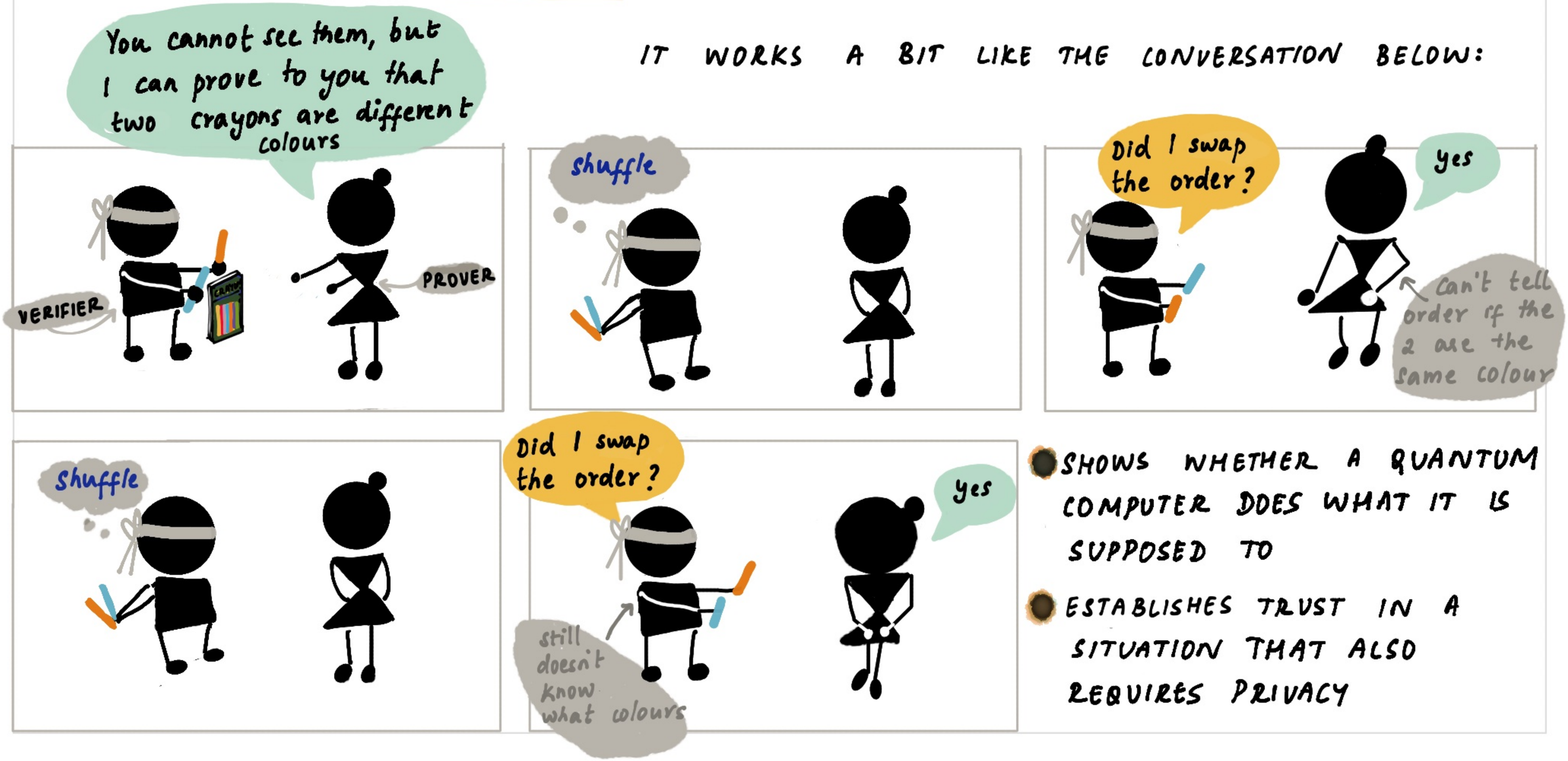


Interactive Proofs for Quantum computation
Apr 2017
D Aharonov
M Ben-or
E Eban
U Mahadev

THE RESULTS OF A QUANTUM COMPUTATION ARE HARD TO PREDICT AS THEY EVOLVE WITH THE LAWS OF QUANTUM MECHANICS. HOW THEN DO WE MEASURE THE SUCCESS OF AN EXPERIMENT/ALGORITHM?

WE USE INTERACTIVE PROOFS TO QUERY THE ALGORITHM IN A STRUCTURED MANNER.

IT WORKS A BIT LIKE THE CONVERSATION BELOW:




- SHOWS WHETHER A QUANTUM COMPUTER DOES WHAT IT IS SUPPOSED TO
- ESTABLISHES TRUST IN A SITUATION THAT ALSO REQUIRES PRIVACY

# THE PRESENT AND FUTURE

— A LITTLE GLIMPSE —

# CURRENT STATE OF AFFAIRS

## QUANTUM SUPREMACY

"WHAT A QUANTUM COMPUTER CAN DO TO MAKE A CALCULATION FASTER (by a few thousand years!) THAN A CLASSICAL COMPUTER"

– JOHN PRESKILL

## EXAMPLE

YEAR : 2019 IN GOOGLE

PROCESSOR : SYCAMORE, 53 QUBITS

TASK : CHECK PATTERN OF A LONG SEQUENCE OF DIGITS

DURATION : AROUND 5 MINUTES

SO? : TO DO THIS VERY TASK SUPERCOMPUTERS TAKE ABOUT 10,000 YEARS!

DISPUTED BY : IBM

See Scott Aaronson's article on this in nytimes.com

## COMPANIES INVESTING IN RESEARCH

IBM

MICROSOFT

RIGETTI

INTEL GOOGLE

AMAZON

HONEYWELL

DWAVE IONQ

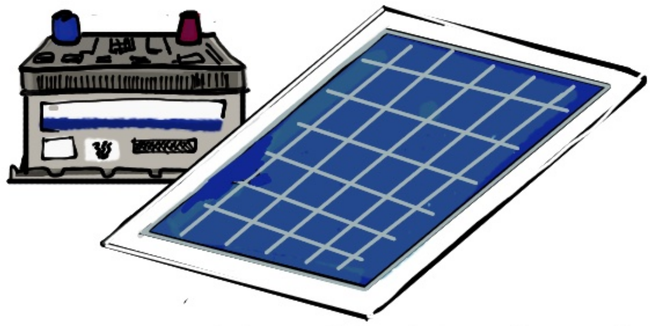
... AND MANY MORE

THE POTENTIAL OF QUANTUM COMPUTERS AND THEIR APPLICATION IS YET TO BE UNDERSTOOD FULLY (AMID ALL THE DEBATE)

# POTENTIAL USES OF QUANTUM COMPUTERS



DRUG RESEARCH



BATTERIES, SOLAR CELLS

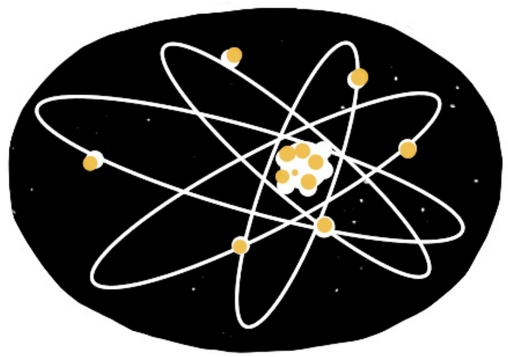


MATERIAL SCIENCE



BREAK CURRENT ENCRYPTION

CREATE NEW ENCRYPTION



SIMULATING

QUANTUM MECHANICS



SOLVING

OPTIMISATION PROBLEMS




MACHINE LEARNING



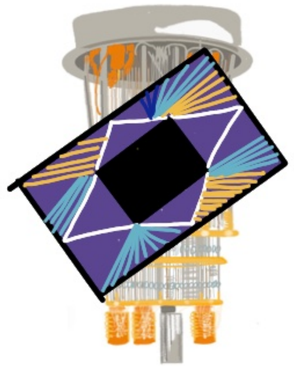
QUANTUM INTERNET



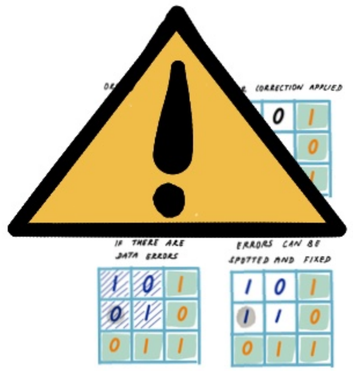
AND MORE!

# WHAT NEXT?

DESPITE THE HYPE, THERE IS MUCH WORK TO BE DONE BEFORE REALISING THE BENEFITS FROM QUANTUM COMPUTERS - IN ENGINEERING AND SOFTWARE DESIGN. AND MORE RESEARCH TO BE DONE IN VARIOUS TOPICS. HERE ARE ONLY A FEW:



HARDWARE FOR QUANTUM COMPUTERS



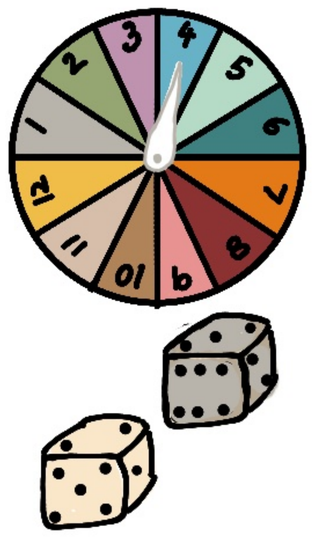

FAULT TOLERANT QUANTUM COMPUTERS

BELL TEST
&
CHSH GAME

QUANTUMNESS TESTS



QUANTUM TELEPORTATION



GENERATING TRUE RANDOM NUMBERS

NOW THAT QUANTUM SUPREMACY HAS BEEN PROVEN, WHAT IS THE FIRST USEFUL THING THAT QUANTUM COMPUTERS CAN DO?

# WOMEN IN QUANTUM COMPUTING

— BECAUSE WE NEED TO KNOW, SHARE AND HONOUR THEIR ACHIEVEMENTS —

AND WHO KNOWS, IT MAY INSPIRE ANOTHER!

# WOMEN IN QUANTUM COMPUTING



## DORIT AHARONOV

MAJOR CONTRIBUTOR TO FOUNDATIONS OF QUANTUM COMPUTATION THEORY

- ENTANGLEMENT
- COMPUTATIONAL COMPLEXITY / QUANTUM ALGORITHMS / INTERACTIVE PROOFS : TESTING
- QUANTUM CRYPTOGRAPHY
- NOISY SYSTEMS / ERRORS / FAULT TOLERANCE



## MICHELLE SIMMONS

DESIGNER OF THE HARDWARE/CHIP FOR THE FIRST 2-QUBIT GATE QUANTUM COMPUTER



## TALIA GERSHON

SPEAKER AND LEAD FOR QUANTUM-COMPUTING-ON-CLOUD TEAM



## BARBARA TERHAL

RESEARCHER OF QUANTUM ERROR CORRECTION AND FAULT TOLERANCE



## STEPHANIE WEHNER

QUANTUM CRYPTOGRAPHER, HACKER, AND BUILDER OF QUANTUM INTERNET

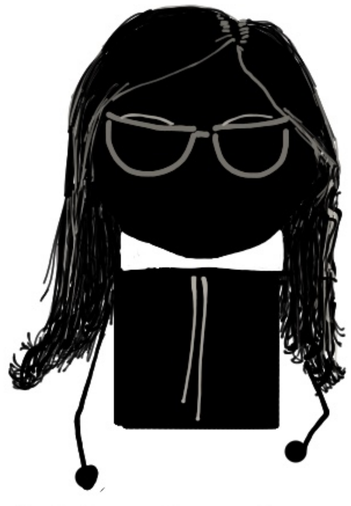
# WOMEN IN QUANTUM COMPUTING

## URMILA MAHADEV



A FIND-OUTER OF WHETHER A QUANTUM COMPUTER DID ANYTHING QUANTUM AT ALL

## CECELIA BOSCHINI



MAKER OF POST-QUANTUM LATTICE BASED-CRYPTO

## MARISSA GIUSTINA



INSTRUCTOR AND QUANTUM COMPUTER BUILDER

## JESSICA POINTING



QUANTUM COMPUTING RESEARCHER/SPEAKER

## EWIN TANG



DEVELOPER OF QUANTUM-INSPIRED EFFICIENT CLASSICAL RECOMMENDATION ALGORITHM

## ELEANOR RIEFFEL



MATHEMATICIAN AND AUTHOR OF QUANTUM COMPUTING: A GENTLE INTRODUCTION

# WOMEN IN QUANTUM COMPUTING

## ELHAM KASHEFI



CO-CREATOR OF
QUANTUM PROTOCOL 200

## ELENI DIAMANTI



QUANTUM COMMUNICATION
RESEARCHER

## URBASI SINHA



HIGHER DIMENSION QUBITS
TRIPLE-SLIT EXPERIMENTER

## TANISHA BASSAN



QUANTUM MACHINE
LEARNING RESEARCHER

## SHELBY KIMMEL



RESEARCHER OF ALGORITHM
EFFICIENCY, ERROR ANALYSIS

## HANHEE PAIK



DESIGNER OF A NEW
SUPER CONDUCTING QUBIT

# MY REFERENCES

**Books**
Quantum: A guide for the perplexed - Jim Al-Khalili
The Quantum World - New Scientist
Quantum Computing Since Democritus - Scott Aaronson

**Online Courses**
Quantum Mechanics & Quantum Computing - Umesh Vazirani, UC Berkeley, YouTube
The Introduction to Quantum Computing - St Petersburg State University, Coursera
Quantum Computing Tutorial - Travis Gritter, YouTube
Understanding Quantum Computers - Future Learn

**Blogs / Websites**
medium.com - Jonathan Hui
ibm.com - What is QC?
technologyreview.com - MIT, Explainer

**Online Talks**
A Beginner's Guide - Talia Gershon
What Quantum Computing isn't - Scott Aaronson, TED
On Complexity and Quantum - Scott Aaronson, YCombinator
On Quantum Computation - John Preskill, YCombinator
QC and Information - Scott Aaronson, Centre for Science of Information
Quantum Computing Reality vs Hype - John Preskill, Caltech
QC and the Entanglement Frontier - John Preskill, UC Berkeley
Einstein Lecture QC Revolution - Michelle Simmons, UNSW
Feynman's Opportunity - Christopher Munroe, Caltech
Crazy History of Quantum Mechanics - Leonard Mlodinow, TED

# MY REFERENCES

**Complexity Theory**
P vs NP - MIT, Explainer
Knowledge, Creativity and P vs NP - Avi Wigderson, math.ias.edu
P vs NP, Efficient Computation - Avi Wigderson, math.ias.edu
The P vs NP problen - Michael Sipser
Lectures Part 1 and 2 - Dorit Aharonov, Dept of Physics Technion
Computational Complexity - Erik Demaine, MIT Open Course Ware

**Church Turing Thesis (CTT)**
CTT: Logical Limit or Breachable Barrier - ACM.org, Jack Copeland, Oron Shagrir

**Programming**
Quantum Computing Languages Landscape QWA, Alba Cervera-Lierta on medium.com

**Testing**
Testing Quantum Devices - Umesh Vazirani, MSRI Math Lovers Forum

**Panel Discussions**
QC: Far Away? Around the Corner? Both? - ACM.org
Beyond Computation P vs NP - Simons Institute

# FOR OTHER TECH STUFF

**More Technology Resources**

**For other illustrated guides and technology and software related resources, please visit thoughtworks.com/insights**

Thank you for reading!