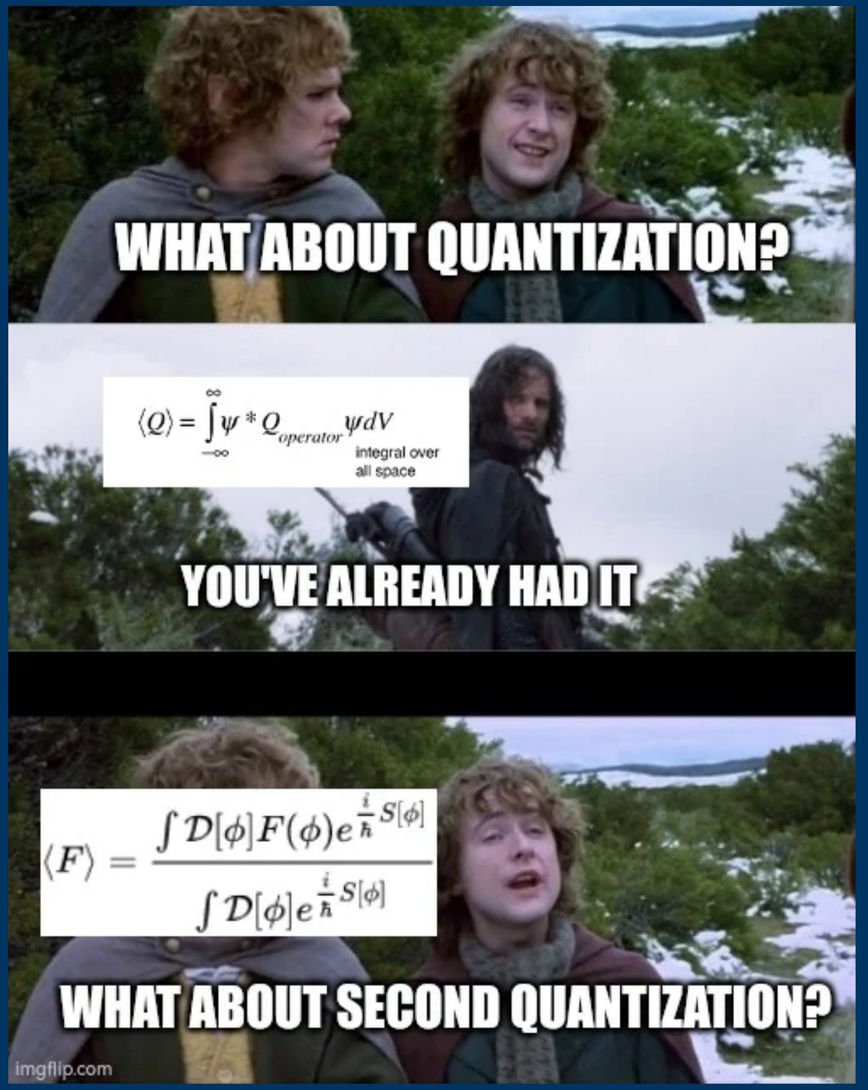
An Armchair Guide:

To Quantum Mechanics



The Armchair Guide

Jonathan Allday

Session 7:

Quantum Snake Oil

Bits and pieces

Classical computing

Relies on processing ‘bits’

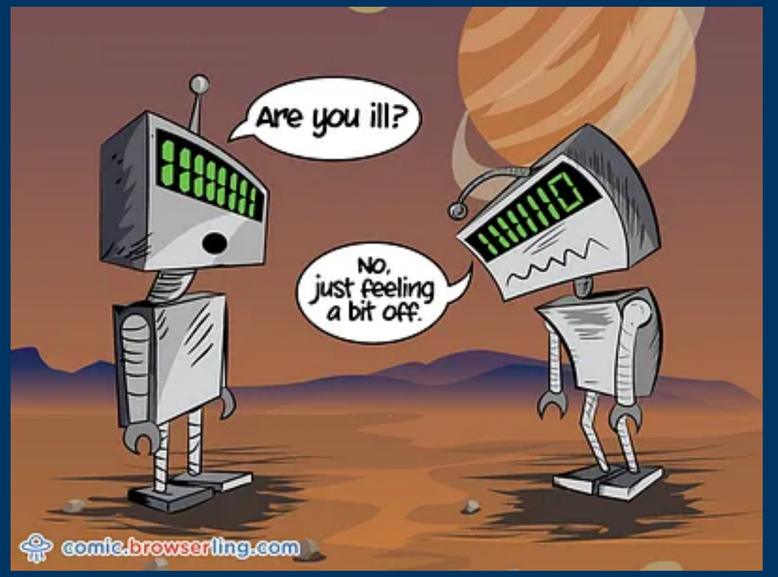
Data broken down into 1s and 0s

Each bit has the value 1 or 0 depending on if it is ‘set’

Process multiple bits (bytes)

Patterns of voltages

1 = 5V; 0 = 0V



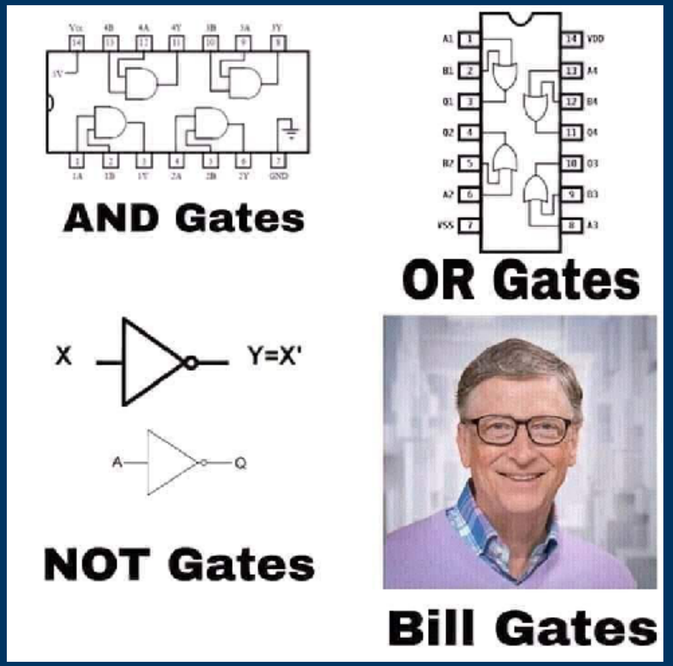
NAND gate…

Short for ‘not’ ‘and’

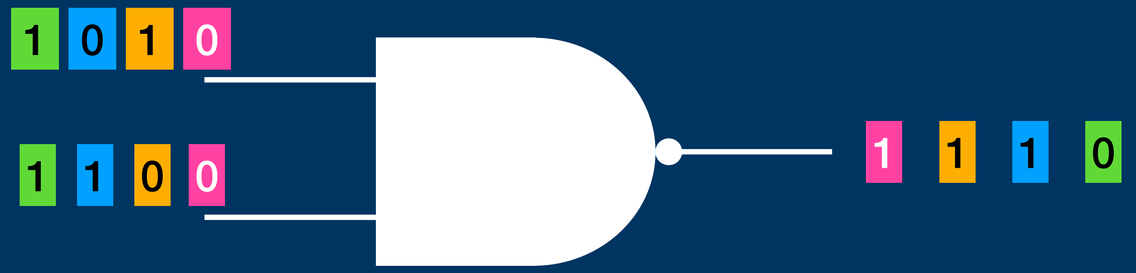
Not an obvious ‘gate’

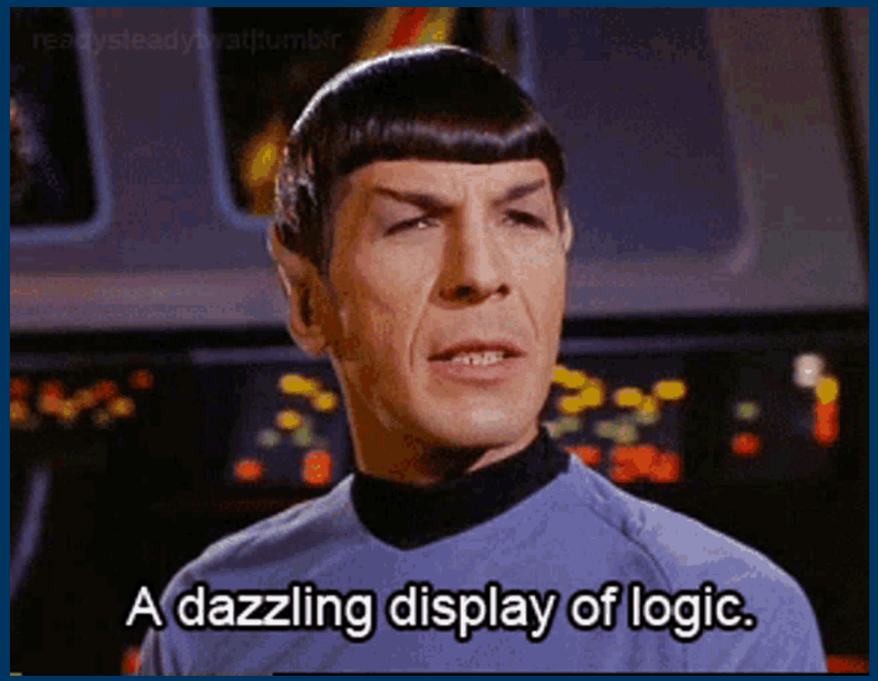
But the easiest to build

Backbone of all other possibilities…



NAND gate…

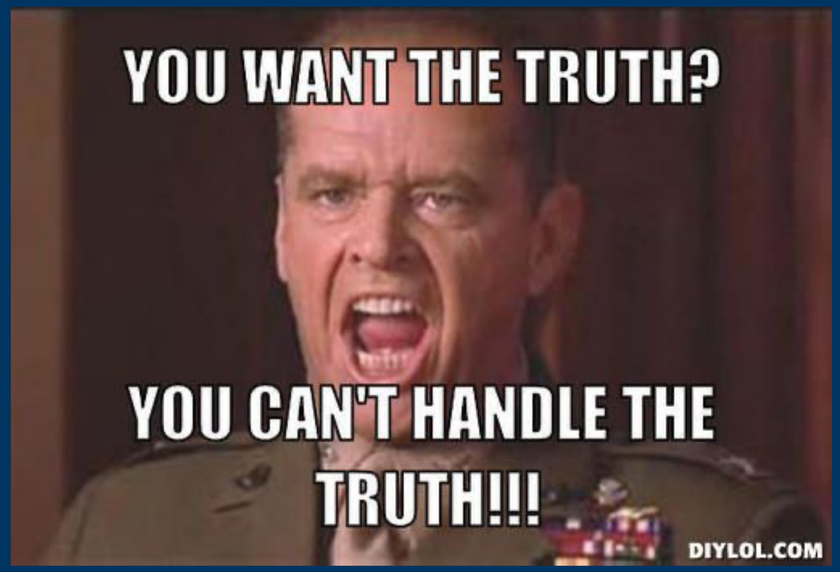




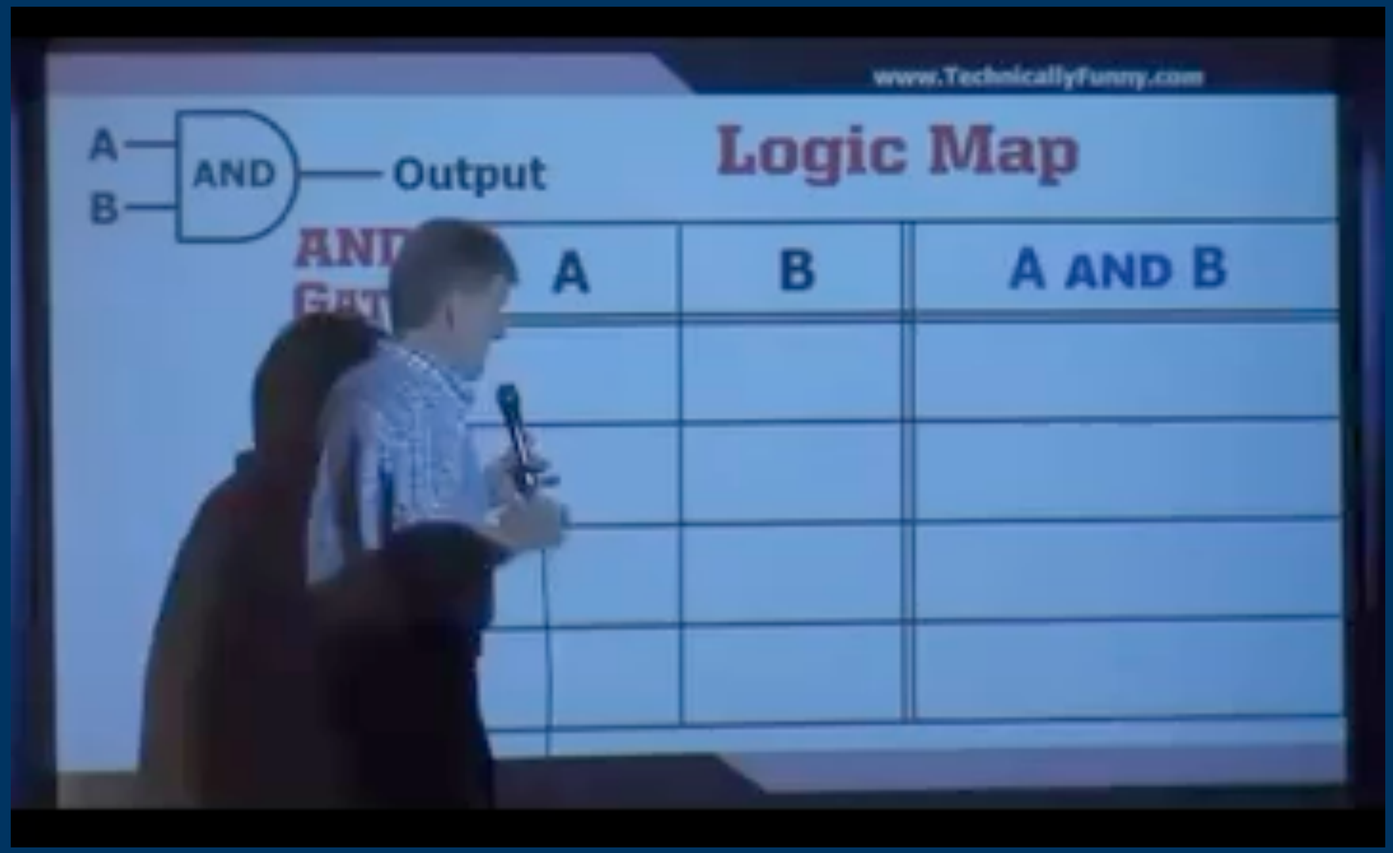
NAND gate…

Truth Table

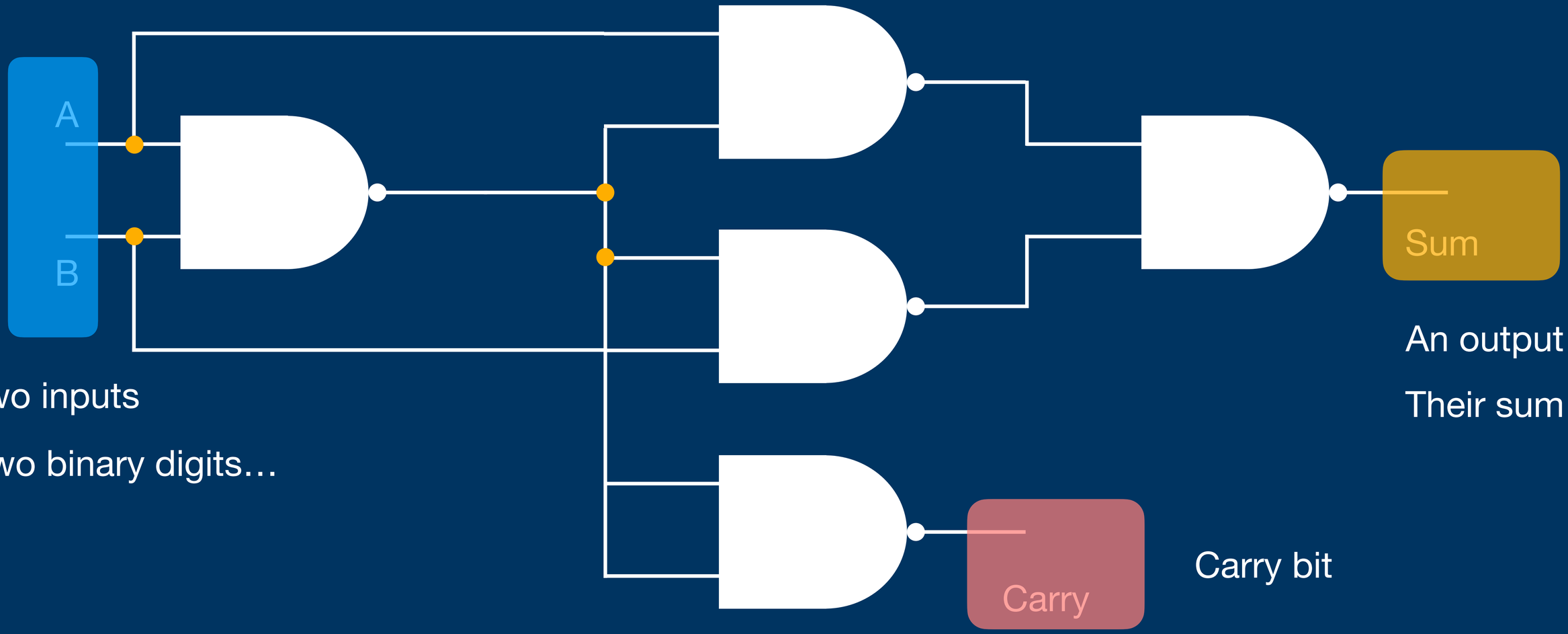
Input		Output
A	B	Q
0	0	1
1	0	1
0	1	1
1	1	0



Marriage gate…



Half adder…



Two inputs

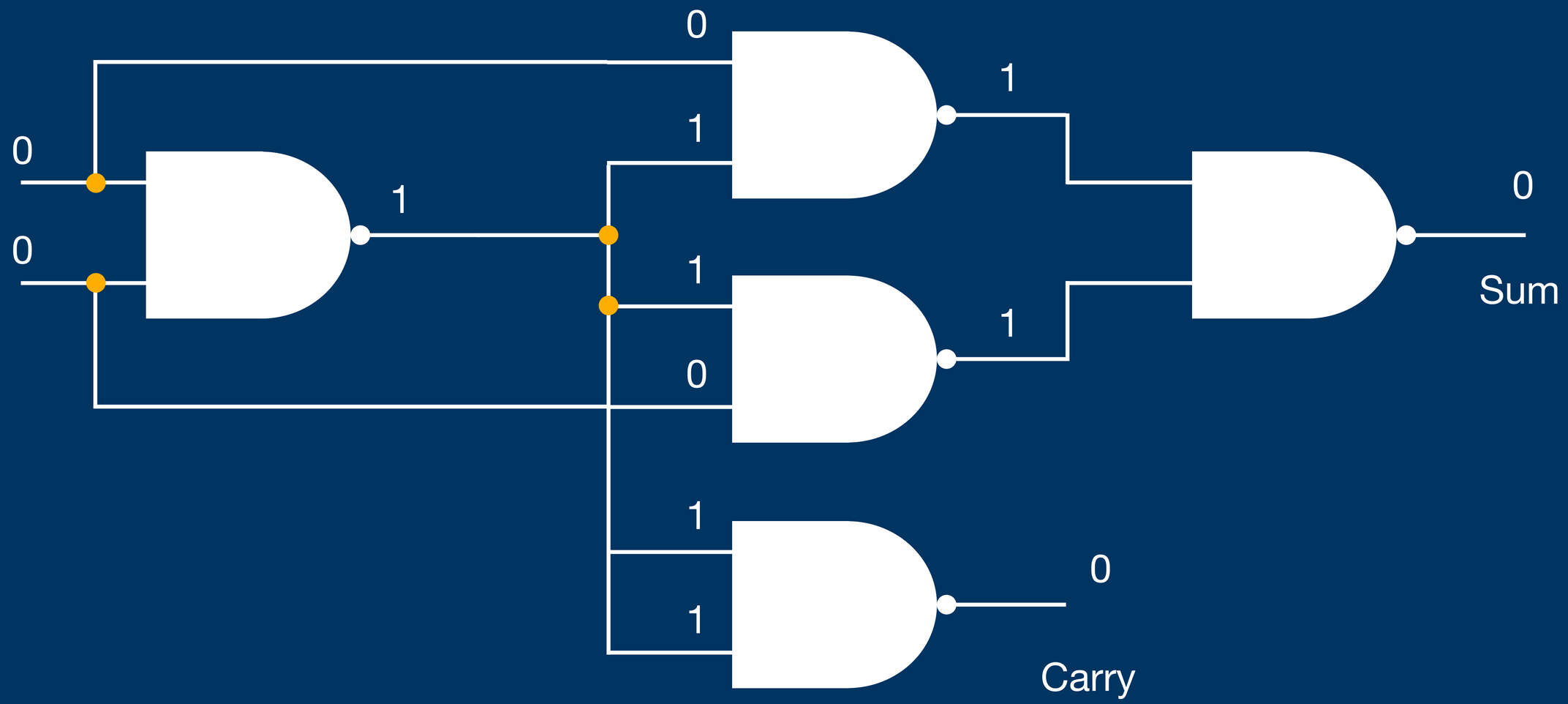
Two binary digits…

An output

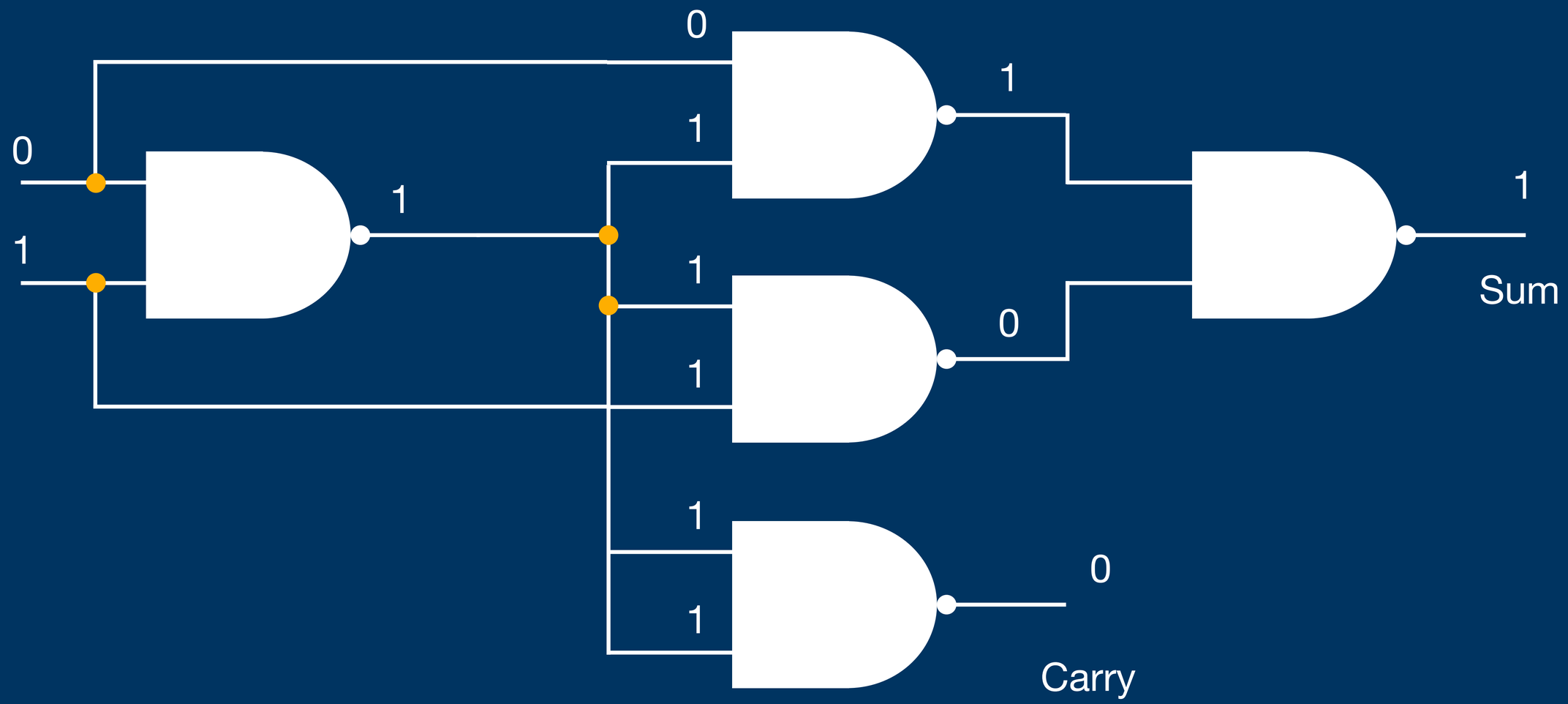
Their sum

Carry bit

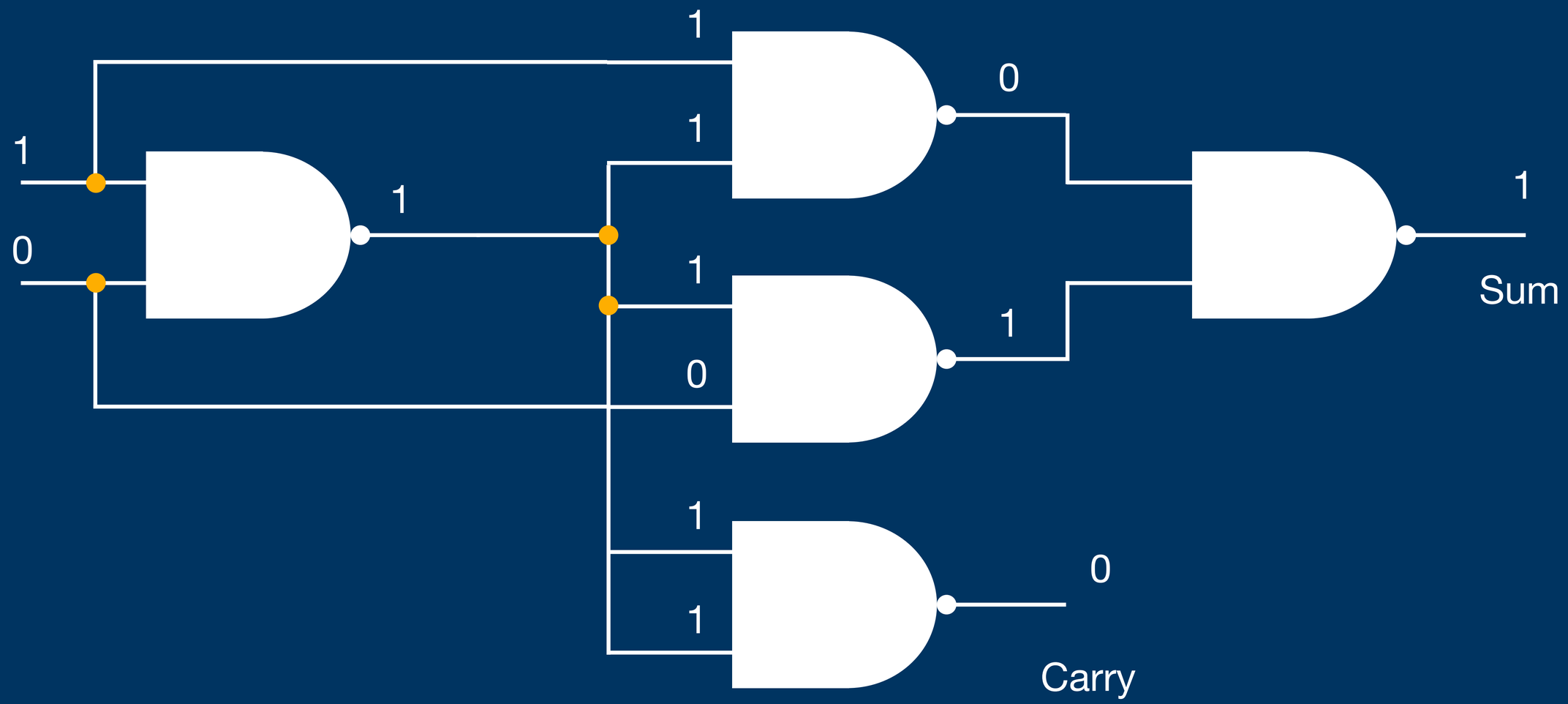
Half adder…



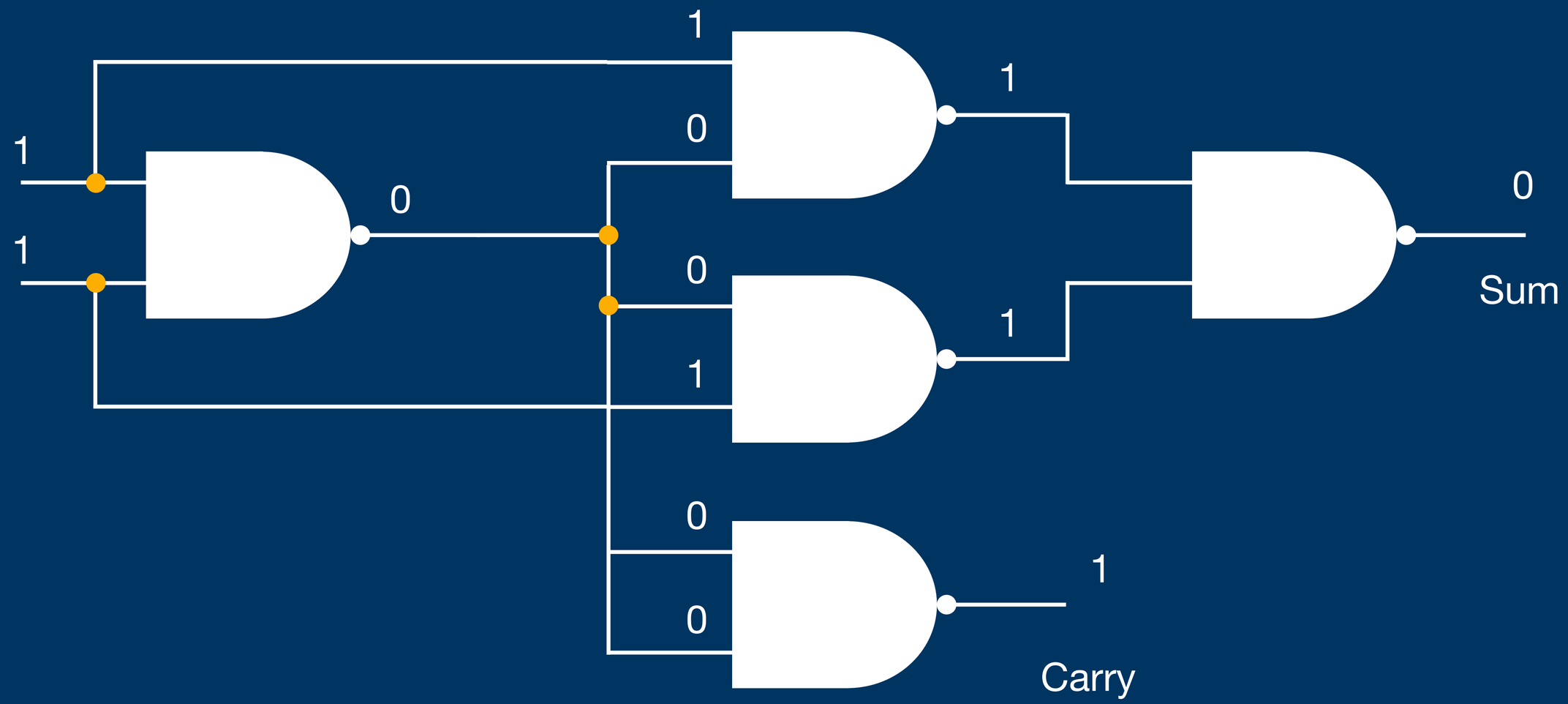
Half adder…

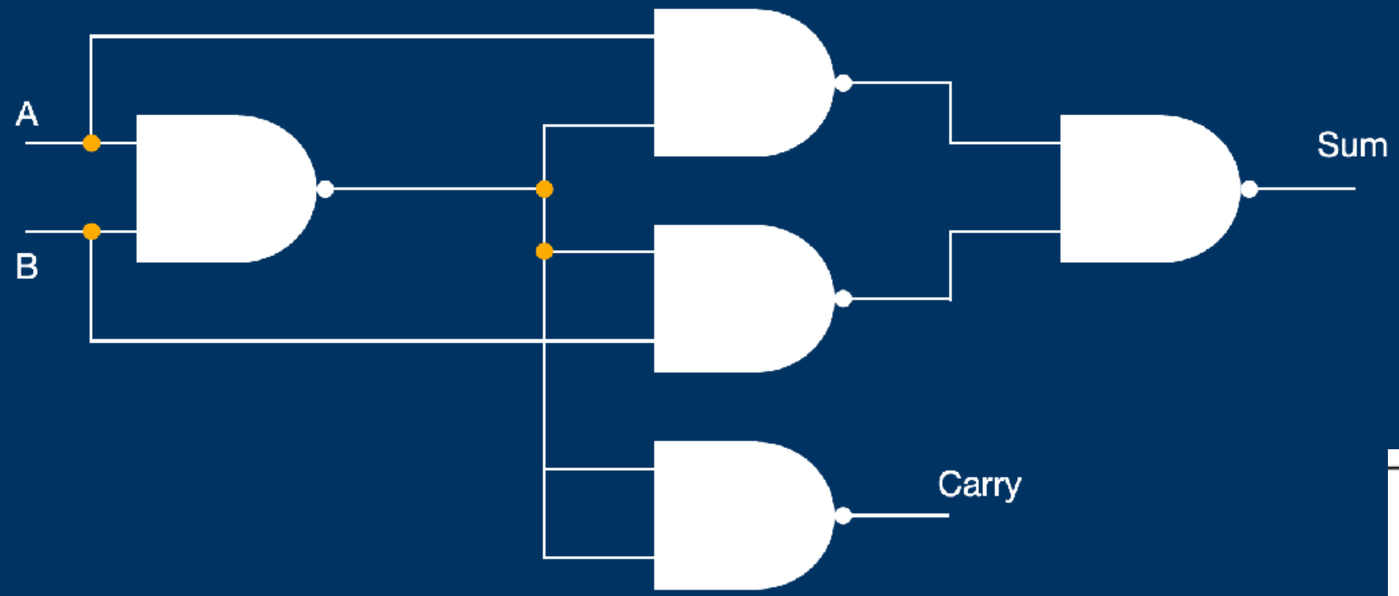


Half adder…



Half adder…

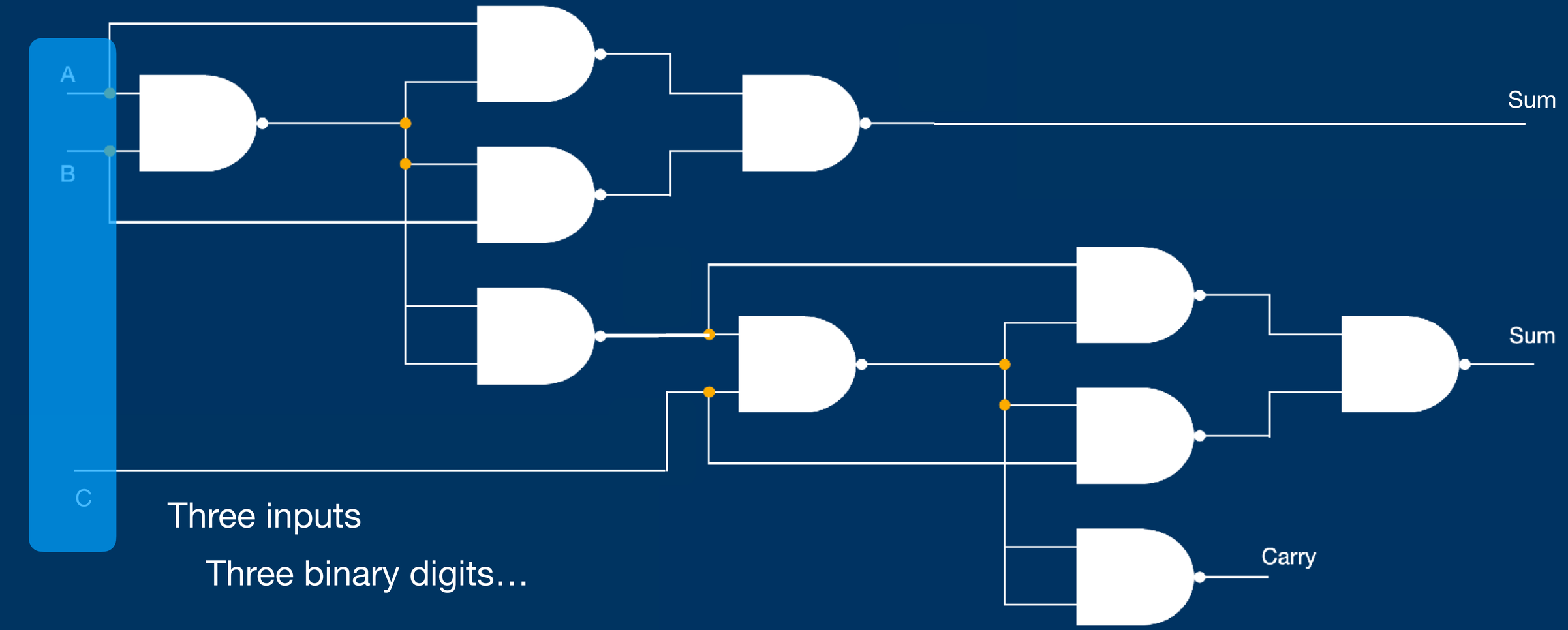




Adding the two bits together

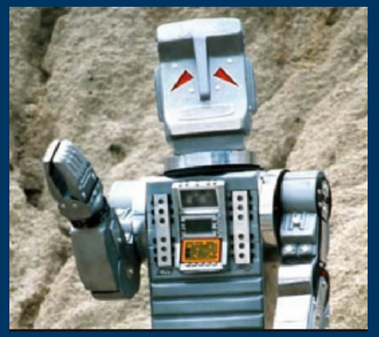
The carry goes to the next adder…

Input		Output	
A	B	Sum	Carry
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1



Three inputs

Three binary digits…



I’ve got this terrible pain in all the diodes down my left side…

Marvin - the paranoid android

Full adder…?

Moore’s law…

No of transistors per chip

Doubles every 2 years

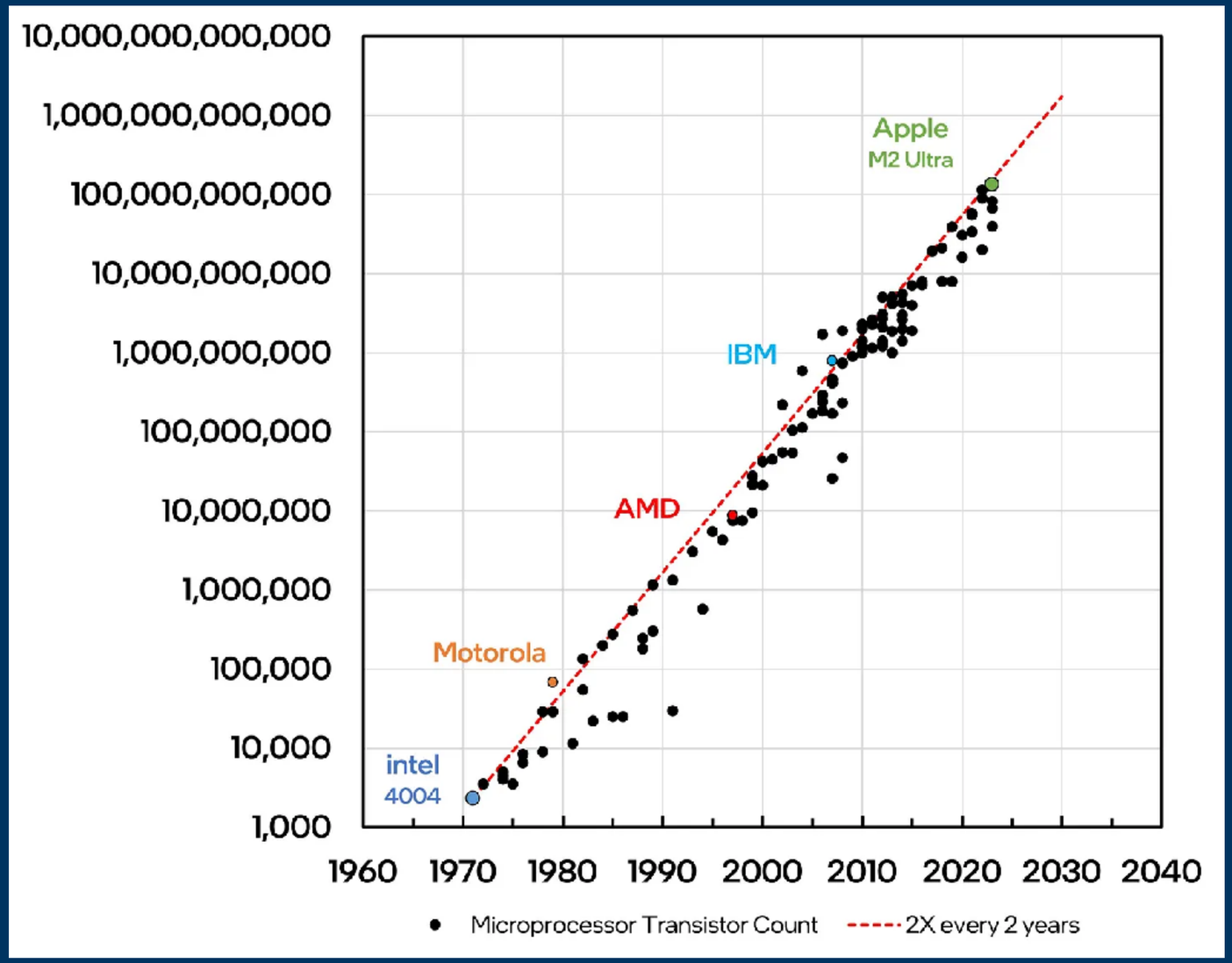
Hence size of a transistor

Heading downwards…

1971 ~ 10 μm

2020 ~ 5 nm

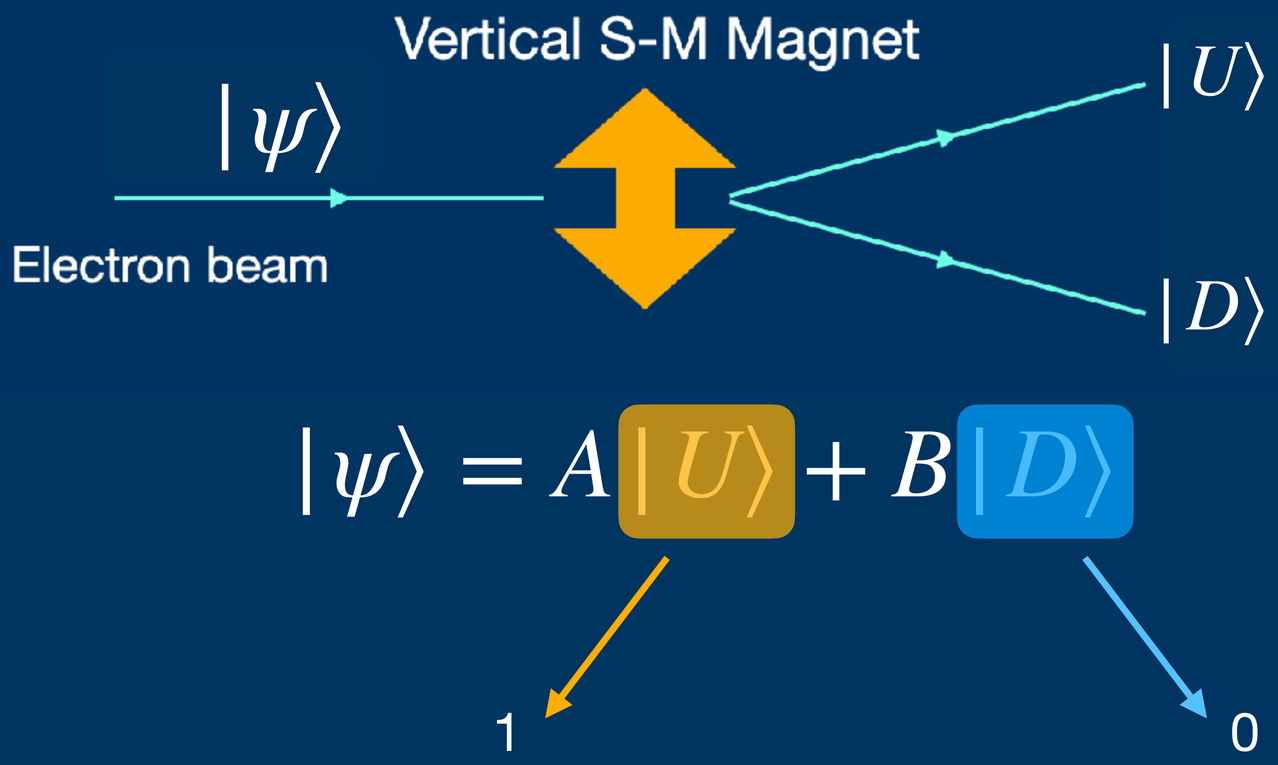
—> atomic scale…



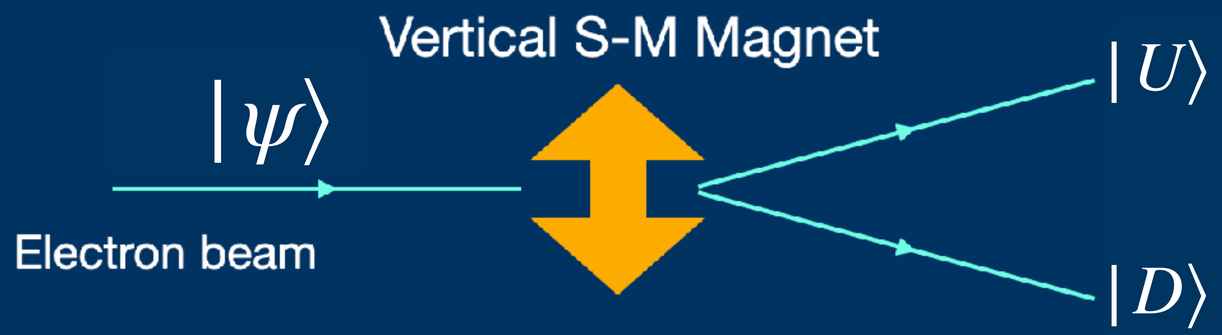
Qubits

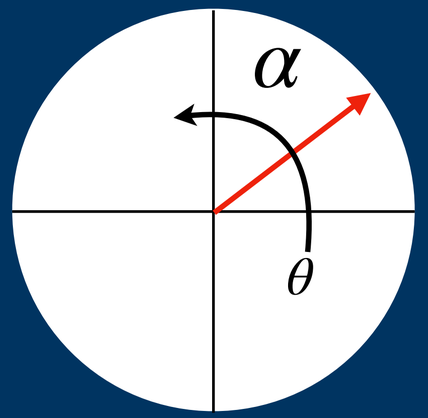
Analogy with a computer bit

A quantum system with two states…



Qubits



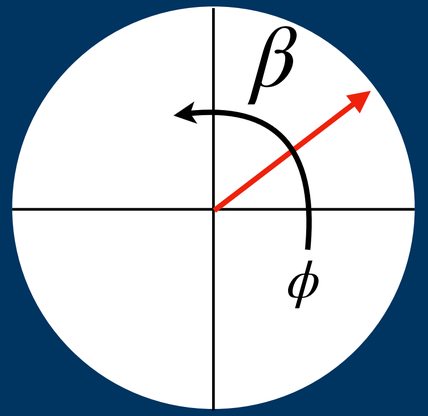


$$A = \alpha e^{i\theta/\hbar}$$

$$|\psi\rangle = A|U\rangle + B|D\rangle$$

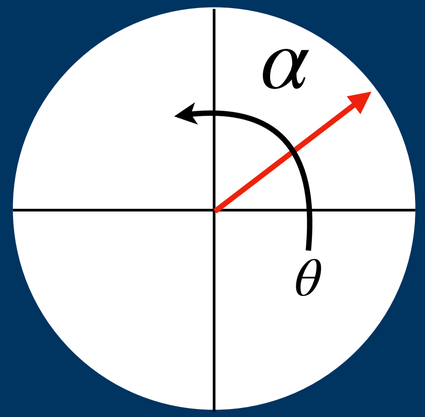
1

0

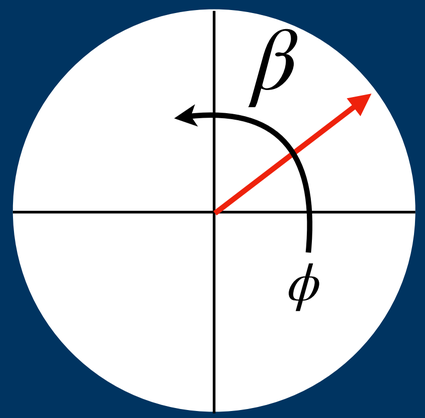


$$B = \beta e^{i\phi/\hbar}$$

Qubits



$$A = \alpha e^{i\theta/\hbar}$$



$$B = \beta e^{i\phi/\hbar}$$

Might think we have 4 numbers to play with…

α and β being two of them…

θ and ϕ being two more…

But…

$$\alpha + \beta = 1$$

Only phase difference matters…

$$\gamma = \phi - \theta$$

Information dense…

Our qubit is…

$$|\psi\rangle = \alpha\,|1\rangle + (1-\alpha)e^{i\gamma}\,|0\rangle$$

However, if can contain a lot of data

n bits of data can go into γ by specifying the angle to n bits….

n bits of data can go into α by specifying the length to n bits….

Result poor

$$|\psi\rangle = \alpha|1\rangle + (1-\alpha)e^{i\gamma}|0\rangle$$

How do you get the information out?

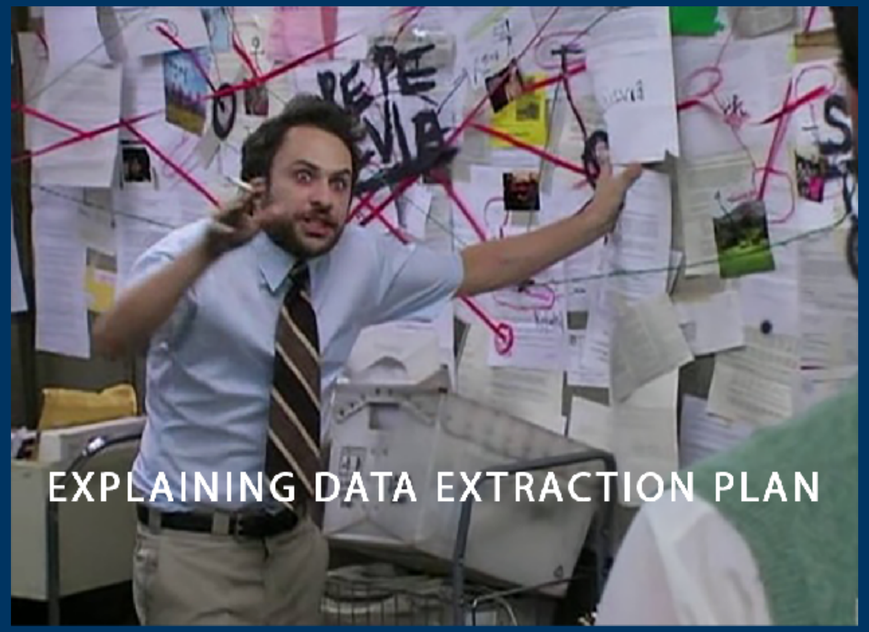
Imagine our qbit is the result of a calculation

Need to get values for α and γ

Measurement only yields

1 0

State collapses…



The needs of the many…

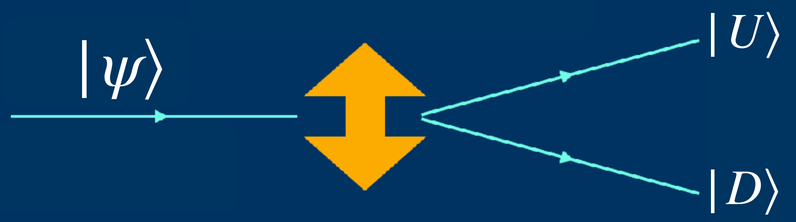
$$|\psi\rangle = \alpha|1\rangle + (1-\alpha)e^{i\gamma}|0\rangle$$

A collection of identical qbits…

Measure using a vertical SG

Make *N* measurements

$$\alpha^2 \approx \frac{\text{no of times we get } |1\rangle}{N}$$



Estimation precision $\sim \frac{1}{\sqrt{N}}$

The needs of the many…

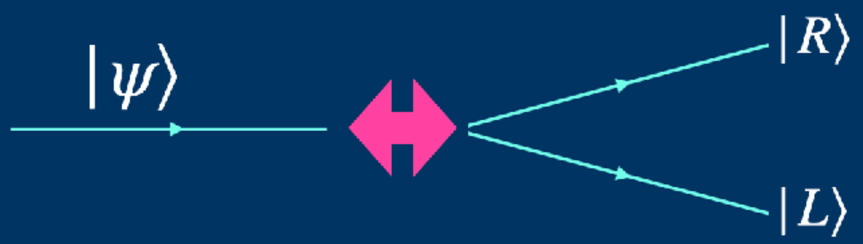
$$|\psi\rangle = \alpha|1\rangle + (1-\alpha)e^{i\gamma}|0\rangle$$

A collection of identical qbits…

Measure using a horizontal SG

Make *N* measurements

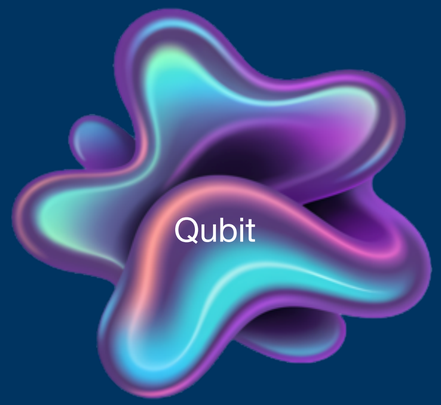
Having already got α you can extract γ



Quantum computation

Prepare a qubit according to a repeatable process

$|\psi\rangle$



Force it to evolve

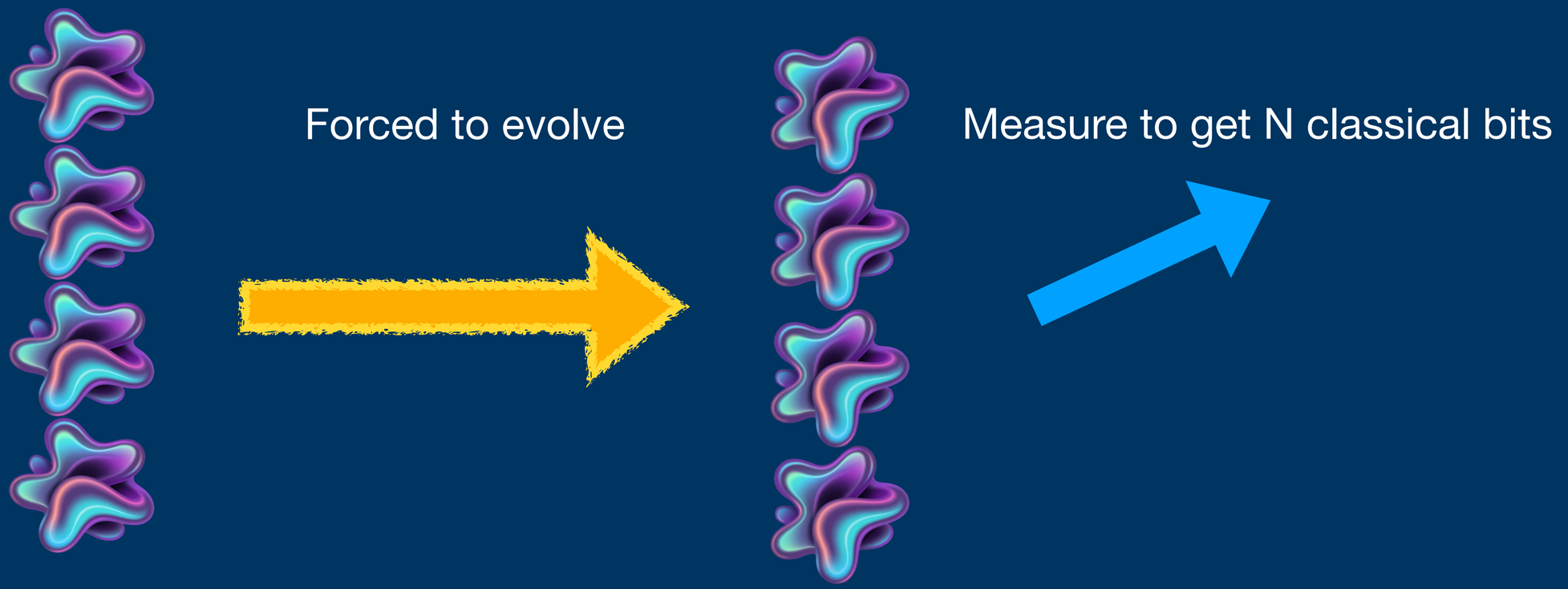
Measure to get 1 classical bit

This is your calculation….

~ 10,000 times per second…

Reset and repeat…

Better…


Forced to evolve
Measure to get N classical bits
N entangled qubits
Reset and repeat…

Best of the best (ish)

IBM Condor

1121 qubits

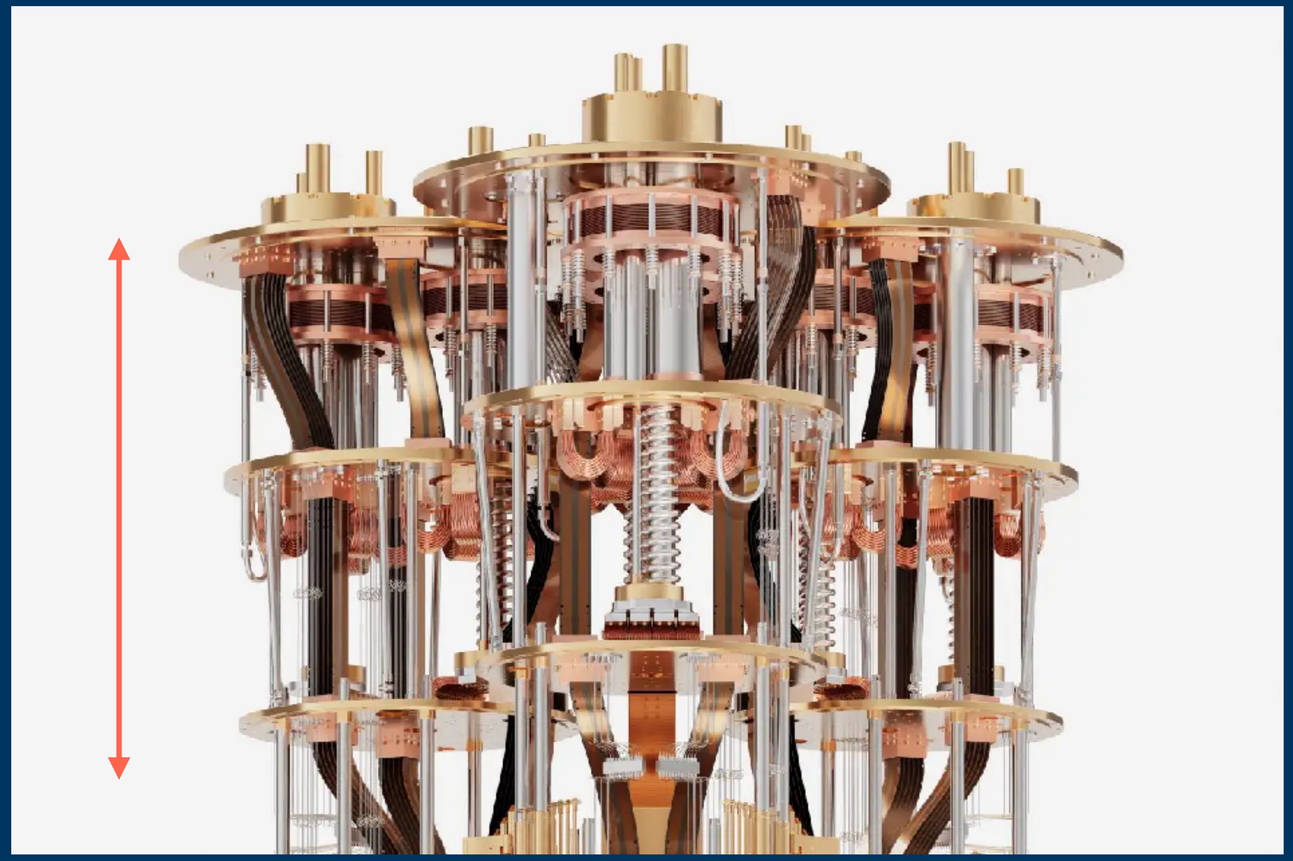
Superconducting atomic junctions

Two lowest energy states of the junction

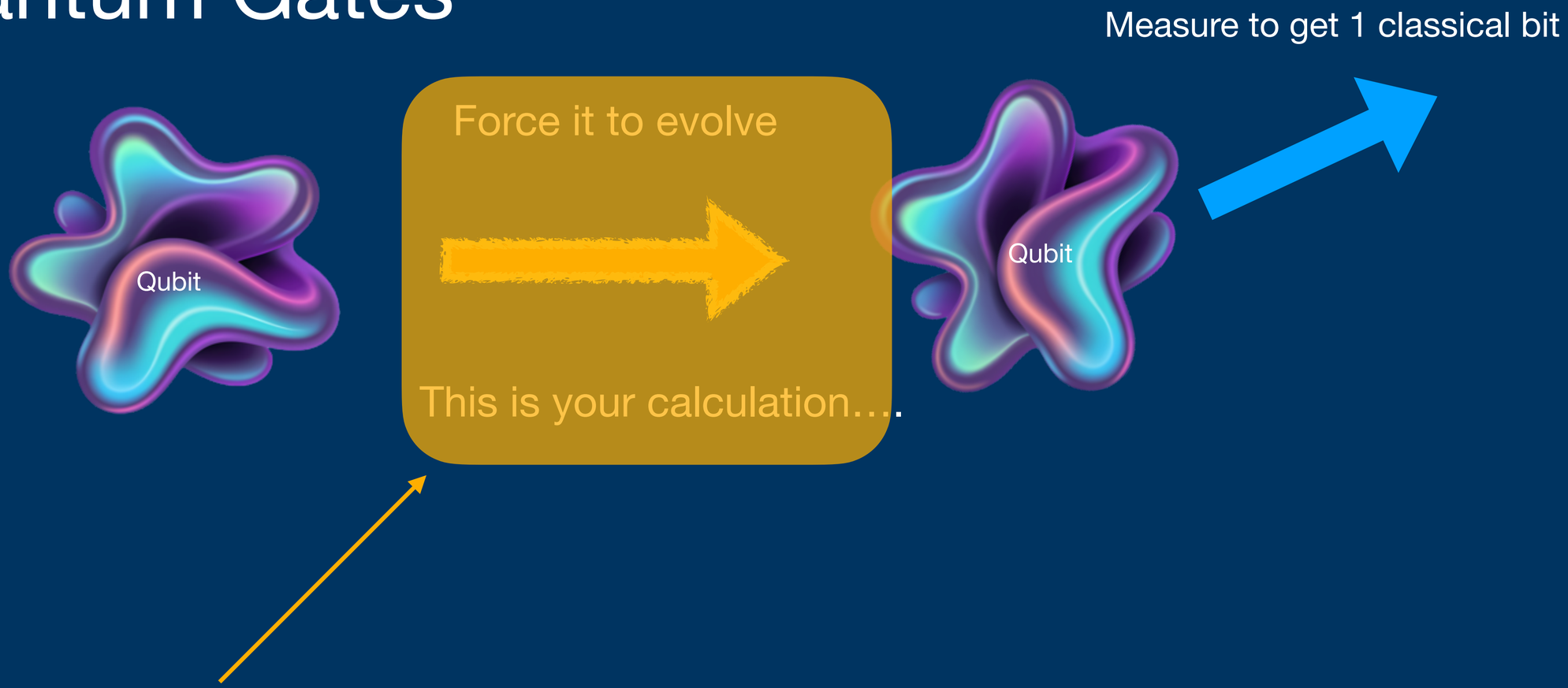
Quantum gates:

Microwave pulses applied to the qubits

Specific frequencies, phases, shapes and timing

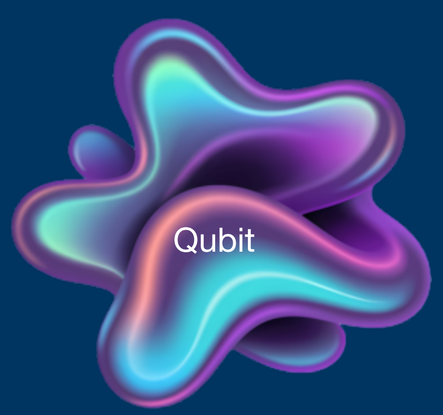


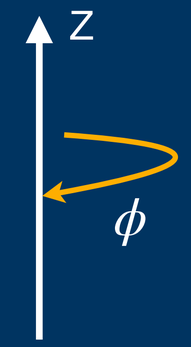
Quantum Gates



Break it down into a set of ‘gates’

Quantum Gates





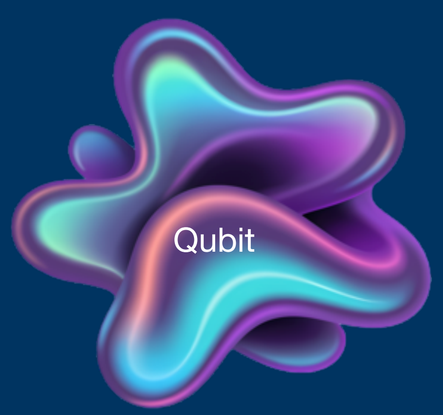
$$\psi = \alpha|1\rangle + \beta e^{i\gamma}|0\rangle$$

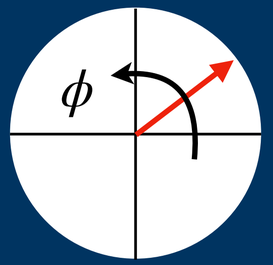
$$\psi = \alpha e^{i\phi/2}|1\rangle + \beta e^{i\gamma}e^{-i\phi/2}|0\rangle$$

X, Y, Z gates

Rotate the state about the axes

Quantum Gates





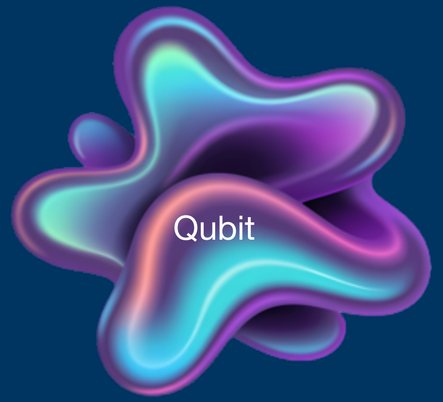
$$\psi = \alpha|1\rangle + \beta e^{i\gamma}|0\rangle$$

$$\psi = \alpha e^{i\phi}|1\rangle + \beta e^{i\gamma}|0\rangle$$

Phase gate

Inserts a relative phase into the qubit

Quantum Gates



$$\psi = \alpha\,|1\rangle + \beta e^{i\gamma}\,|0\rangle$$

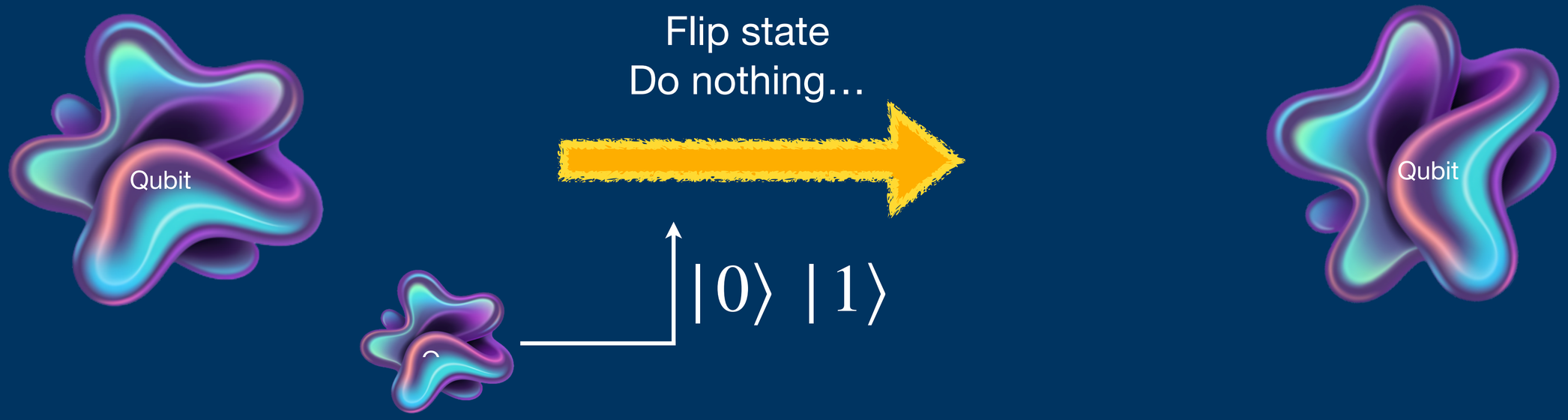
$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$\psi = \frac{1}{\sqrt{2}}\left[(\beta e^{i\gamma} - \alpha)\,|1\rangle + (\beta e^{i\gamma} + \alpha)\,|0\rangle\right]$$

Hadamard gate

Kind of generally fiddles with things….

Quantum Gates



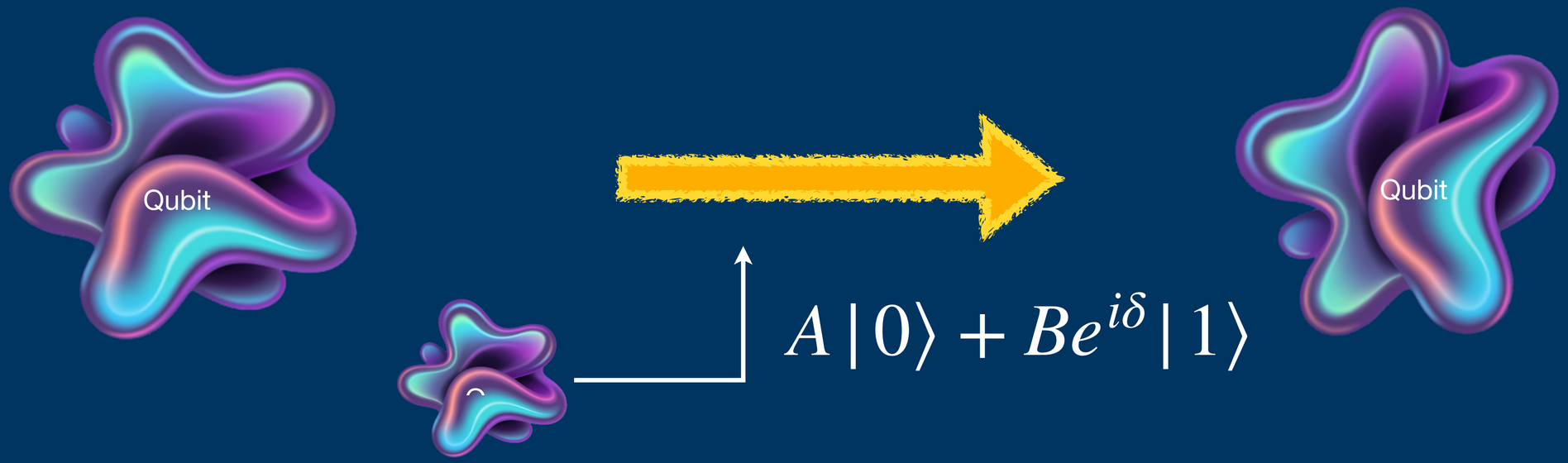
$$\Psi = \alpha|0\rangle|1\rangle + \beta e^{i\gamma}|0\rangle|0\rangle \Rightarrow \Psi = \alpha|0\rangle|1\rangle + \beta e^{i\gamma}|0\rangle|0\rangle$$

$$\Psi = \alpha|1\rangle|1\rangle + \beta e^{i\gamma}|1\rangle|0\rangle \Rightarrow \Psi = \alpha|1\rangle|0\rangle + \beta e^{i\gamma}|1\rangle|1\rangle$$

CNOT gate

Acts on one qubit according to the state of another

Quantum Gates

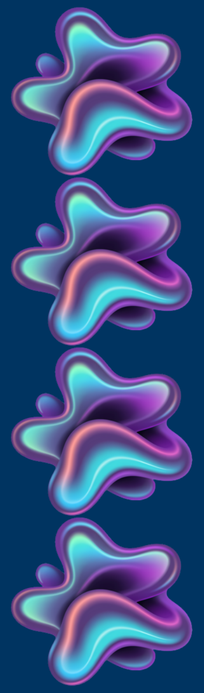


If control qubit is in a superposition…

CNOT entangles the qubits…

$$A\alpha|0\rangle|1\rangle + \beta e^{i\delta}|0\rangle|1\rangle + A\beta e^{i\delta}|1\rangle|1\rangle + \beta B e^{i(\delta+\gamma)}|1\rangle|0\rangle$$

So…



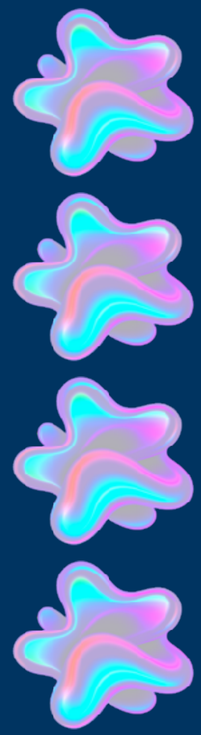
N entangled qubits

Sequence of gates

This forms our ‘programme’

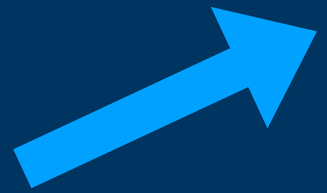
Or algorithm

New state



N entangled qubits

Measure to get N classical bits



Example…

Evaluate a statement:

a AND NOT b

Conventionally, evaluate a row at a time…

a	b	NOT b	a AND NOT b
F	F	T	F
T	F	T	T
F	T	F	F
T	T	F	T

Quantum Computer

$$F = |0\rangle \; T = |1\rangle$$

One qubit for each variable

Set to F

$$|\ldots\phi\ldots\rangle \; |0\rangle|0\rangle\ldots|0\rangle \; |0\rangle$$

One qubit for the result

Another sequence is the query being evaluated

a	b	NOT b	a AND NOT b
F	F	T	F
T	F	T	T
F	T	F	F
T	T	F	T

Quantum Computer

a	b	NOT b	a AND NOT b
F	F	T	F
T	F	T	T
F	T	F	F
T	T	F	T

Apply Hadamard gate to first qubit…

$$|\ldots\phi\ldots\rangle\,|0\rangle\,|0\rangle\ldots|0\rangle$$

$$|\ldots\phi\ldots\rangle\,\frac{1}{\sqrt{2}}\left[|1\rangle+|0\rangle\right]|0\rangle\ldots|0\rangle\,|0\rangle$$

Apply to each qubit in turn

until the sequence is an entanglement of each qubit in a superposition of T/F

Quantum Computer

a	b	NOT b	a AND NOT b
F	F	T	F
T	F	T	T
F	T	F	F
T	T	F	T

$$|\ldots\phi\ldots\rangle \quad |1/0\rangle|1/0\rangle\ldots|1/0\rangle \quad |0\rangle$$

Becomes an entanglement of all the row answers…

Then run the ‘code’ that evaluates all possibilities in one go…

Cool….

But… how do you get the answer out?

Any measurement collapses the entanglement

Just gives the answer for one row…

Rinse and repeat…

No better than conventional…

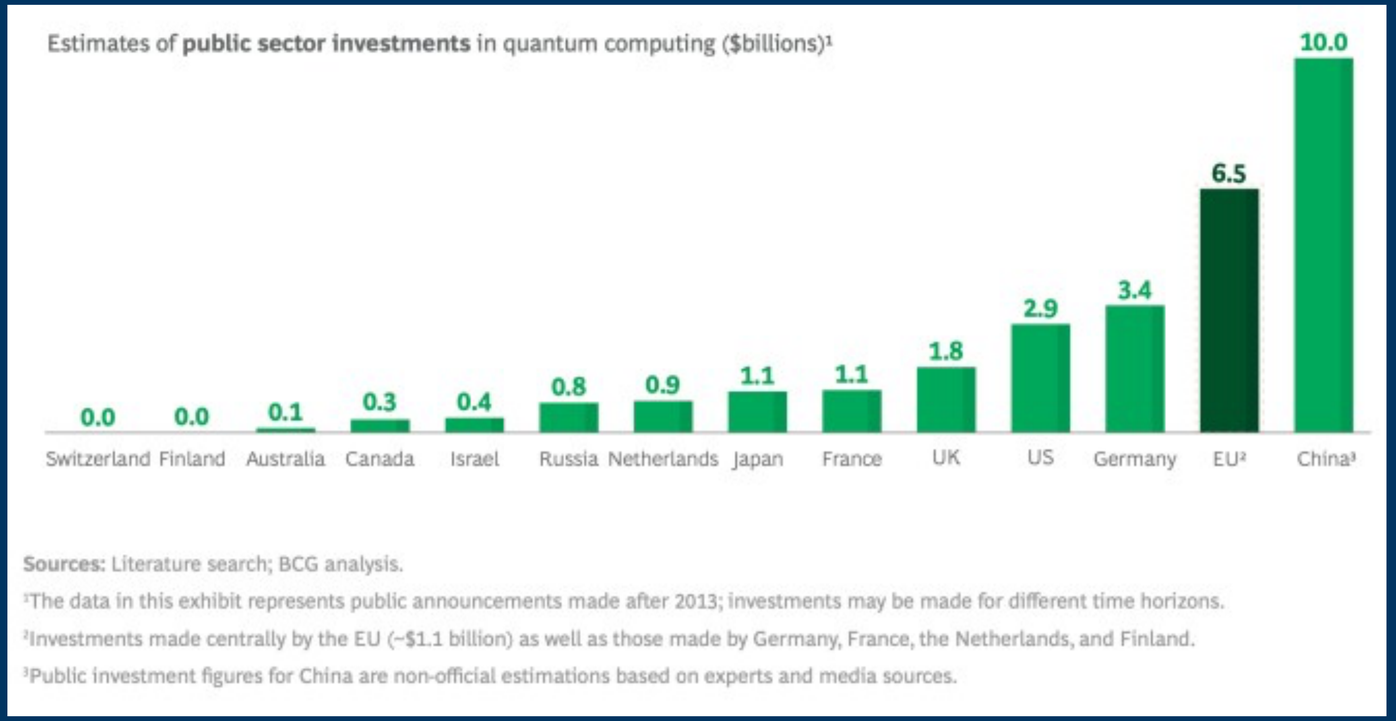
Scott Aaronson

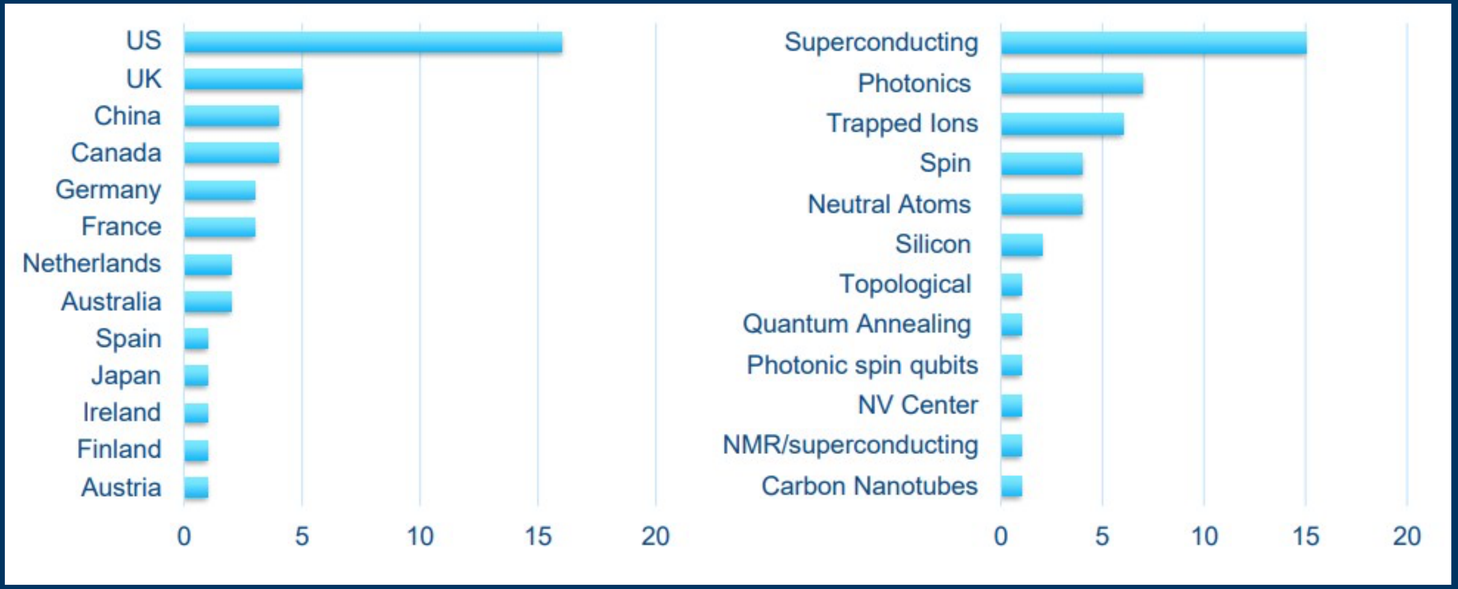
If you take nothing else from this blog: quantum computers won't solve hard problems instantly by just trying all solutions in parallel.

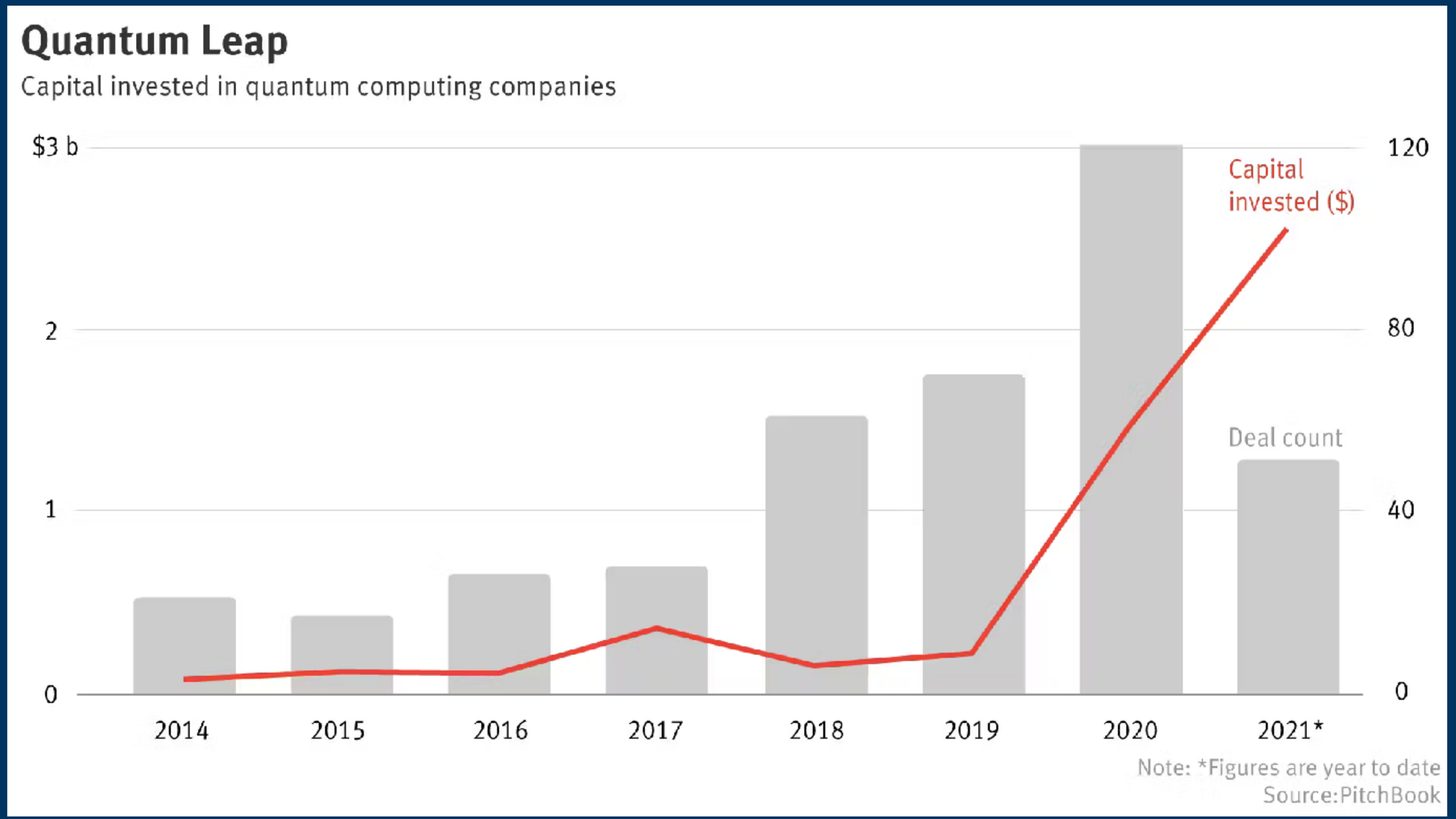
The goal in devising an algorithm for a quantum computer is to choreograph a pattern of constructive and destructive interference so that for each wrong answer the contributions to its amplitude cancel each other out, whereas for the right answer the contributions reinforce each other. If, and only if, you can arrange that, you'll see the right answer with a large probability when you look.

https://scottaaronson.blog/

How do we do that?


Estimates of public sector investments in quantum computing ($billions)[1]
0.0
0.0
0.1
0.3
0.4
0.8
0.9
1.1
1.1
1.8
2.9
3.4
6.5
10.0
Switzerland
Finland
Australia
Canada
Israel
Russia
Netherlands
Japan
France
UK
US
Germany
EU[2]
China[3]
Sources: Literature search; BCG analysis.
[1]The data in this exhibit represents public announcements made after 2013; investments may be made for different time horizons.
[2]Investments made centrally by the EU (~$1.1 billion) as well as those made by Germany, France, the Netherlands, and Finland.
[3]Public investment figures for China are non-official estimations based on experts and media sources.


US
UK
China
Canada
Germany
France
Netherlands
Australia
Spain
Japan
Ireland
Finland
Austria
0
5
10
15
20
Superconducting
Photonics
Trapped Ions
Spin
Neutral Atoms
Silicon
Topological
Quantum Annealing
Photonic spin qubits
NV Center
NMR/superconducting
Carbon Nanotubes
0
5
10
15
20


Quantum Leap
Capital invested in quantum computing companies
$3 b
2
1
0
120
80
40
0
Capital invested ($)
Deal count
2014
2015
2016
2017
2018
2019
2020
2021*
Note: *Figures are year to date
Source:PitchBook

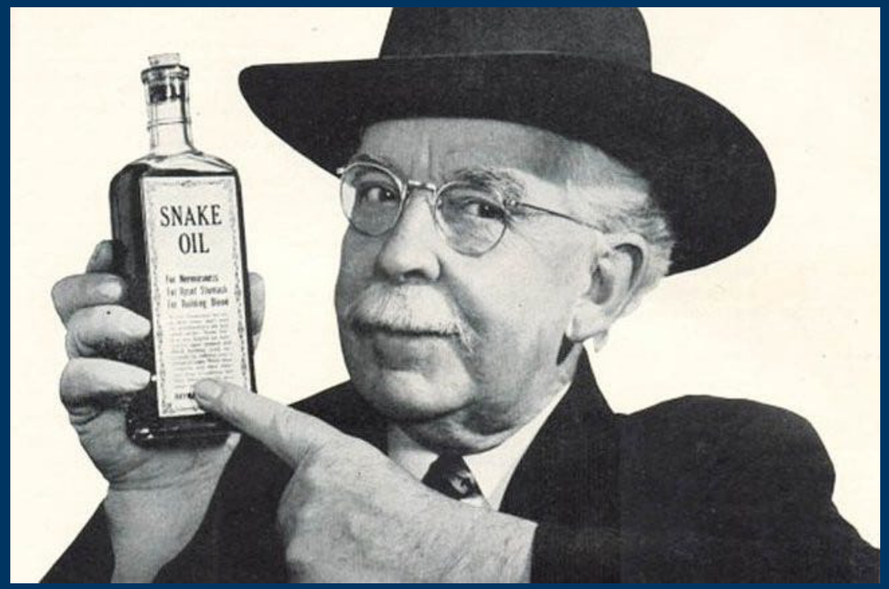
Snake Oil…

No general proof

That a quantum computer must

Be faster than a digital

In all situations



Believe it or not…

But…

Shor’s factoring algorithm

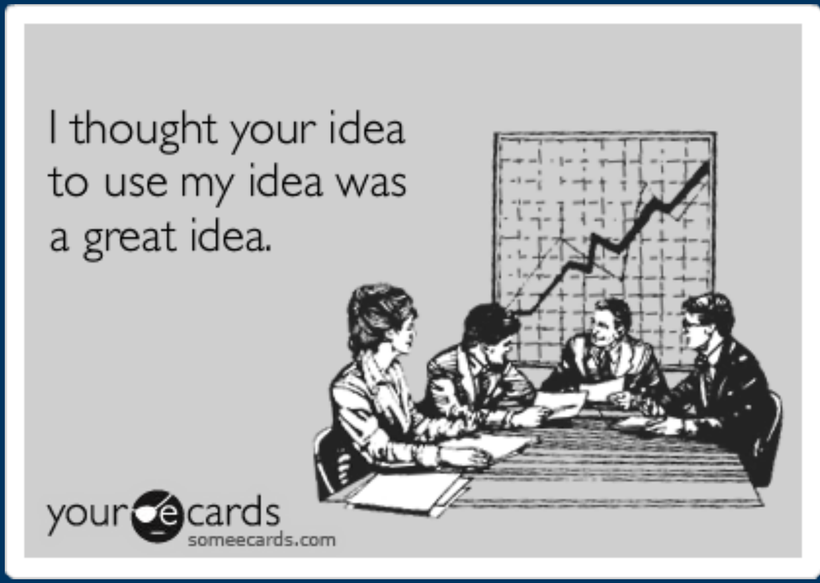
Breaks a number into prime factors

$$84 = 2 \times 42$$

Prime Not prime…

$$84 = 2 \times 2 \times 3 \times 7$$

All prime…



But…

N=135066410865995223349603216278805969938881475605667027524485143851526510604859533833940287150571909441798207282164471551373680419703964917430464965892742562393410208643832021103729587257623585096431105640735015081875106765946292055636855294752135008528794163773285339061097505443349998111500569772368909275 63

2.2 GHz Athlon 64 CPU PC with ≤ 2 GB memory

2 years…

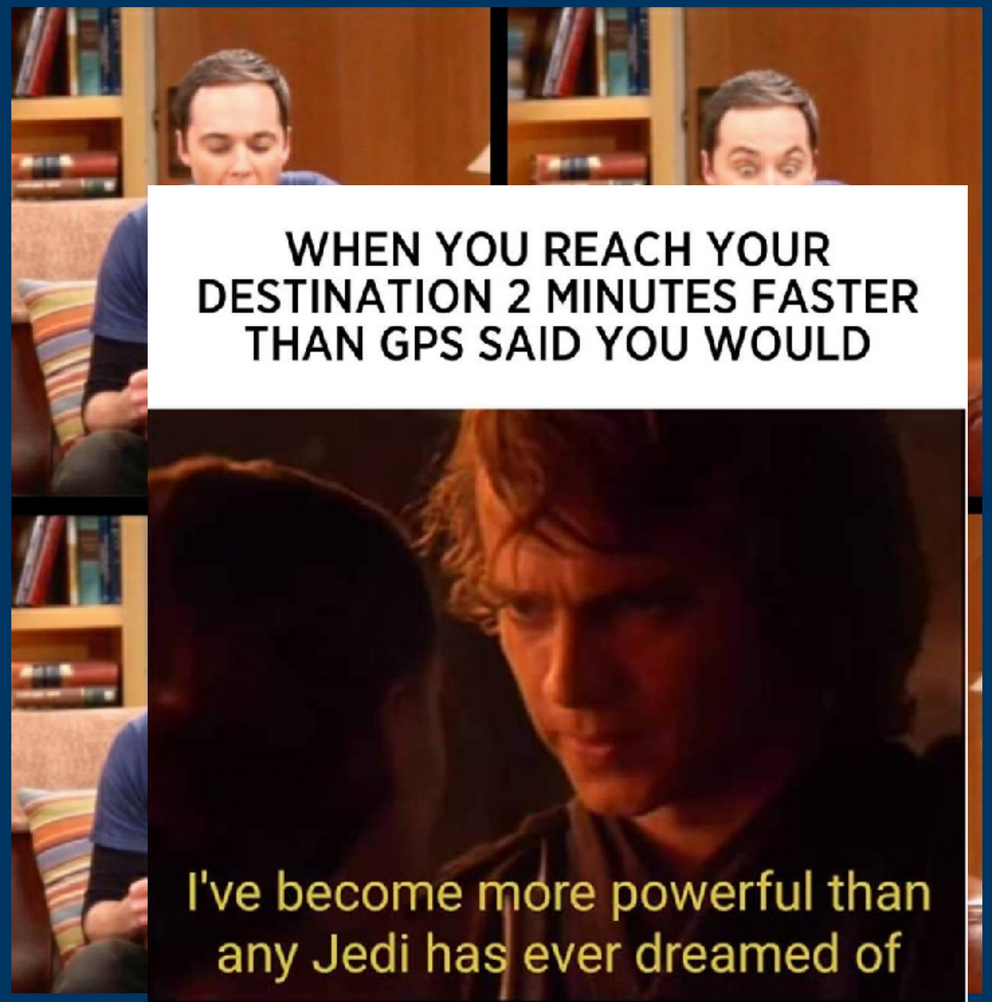
Why does it matter???

Factoring large numbers:

The key to cracking RSA and other encryption…

Shor’s factoring algorithm

Exponentially faster than a digital computer



But…

2001 - IBM team

7 qubit device

Nuclear magnetic resonance

Successfully factored….

$$15 = 3 \times 5$$

Best so far, fully using the algorithm

$$21 = 3 \times 7$$

But…

Qubit has to be screened from the environment

That decoherence again…

So:

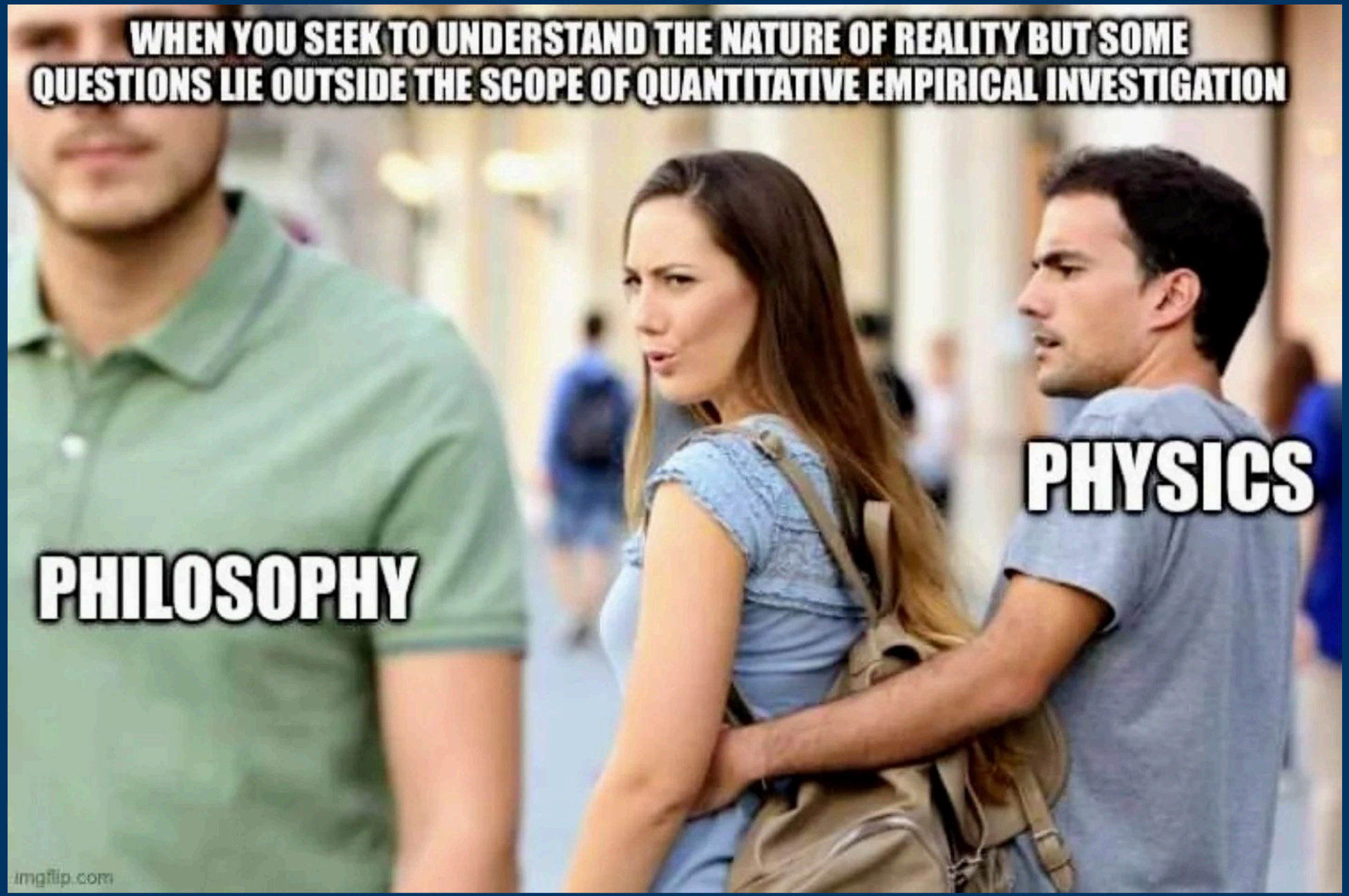
Let the engineers play

Can do some physics with what they create

Study shielded quantum systems

Also:

Exposes more people to the nature of quantum reality…


WHEN YOU SEEK TO UNDERSTAND THE NATURE OF REALITY BUT SOME QUESTIONS LIE OUTSIDE THE SCOPE OF QUANTITATIVE EMPIRICAL INVESTIGATION
PHILOSOPHY
PHYSICS
imgflip.com