Quantum Computing

for “classical” developers

Julian Burr @ DDD Brisbane 2024

BRISBANE

PLATINUM

Octopus Deploy

GOLD

Insight

PATIENT ZERO

VALD

SILVER

NDC { Sydney }

pinch

STANDARD

LMG

Seq

SixPivot

Telstra Purple

CHILDCARE

Octopus Deploy

COFFEE

LMG

Telstra Purple

DIVERSITY/ HARDSHIP

SixPivot

MEDIA

SOULSOLUTIONS

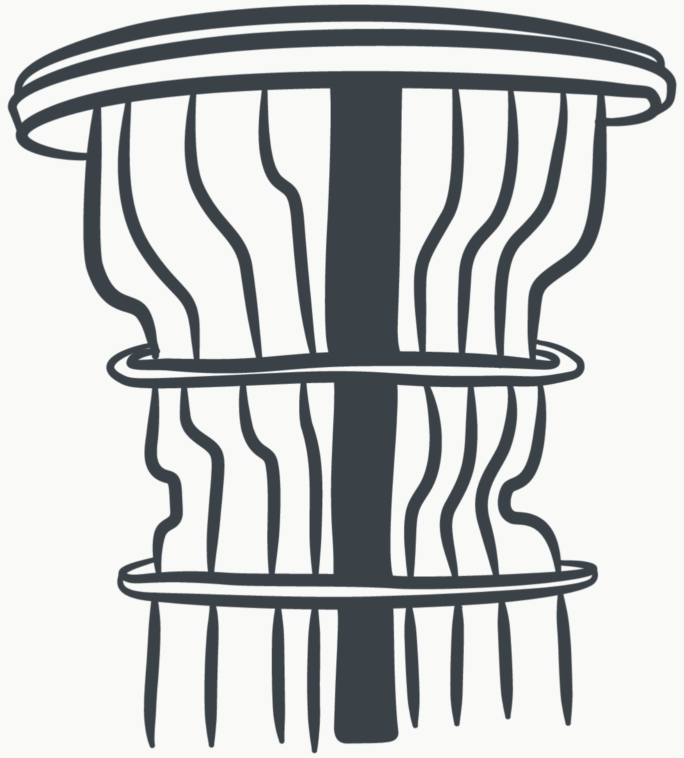
LUNCH

PATIENT ZERO

Intro: Key takeaway

“Classical” Computer

is being replaced by

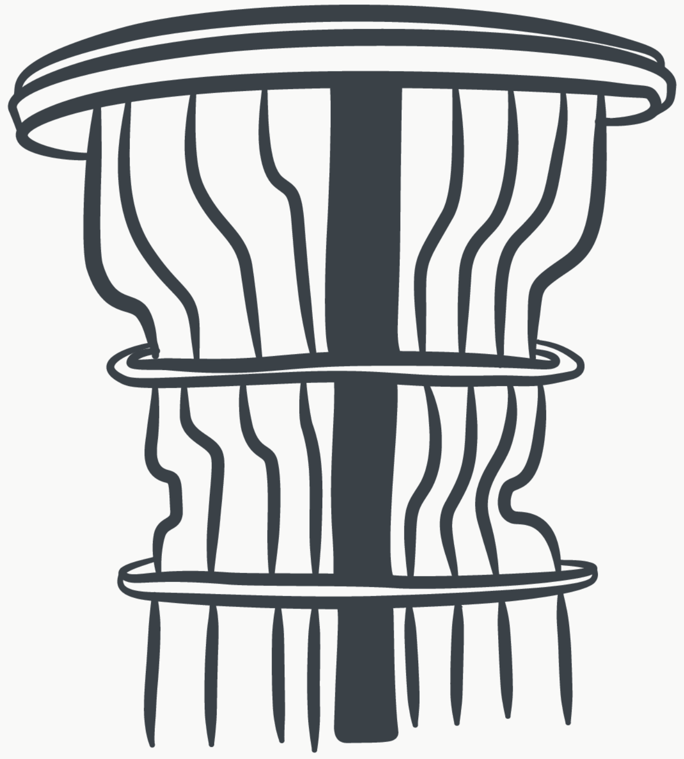


Quantum Computer

Intro: Key takeaway

"Classical" Computer

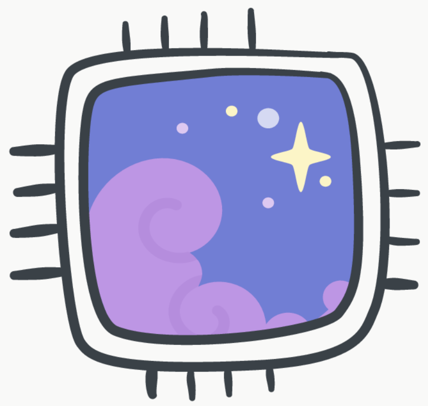
is being **enhanced** by



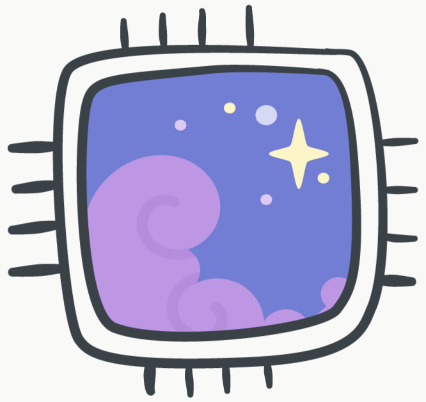
Quantum Computer

"Classical" Computer

is being **enhanced** by



Quantum Processing Unit (QPU)

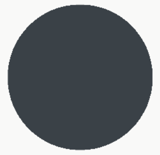


Quantum Processing
Unit (QPU)

"Classical"
Computer

Part I: Quantum computing fundamentals

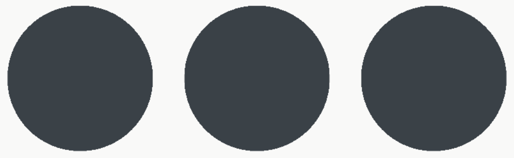
"Classical" bit vs. "Quantum" bit



“Classical” bit

Can be in one of two possible states, 0 or 1

n "classical" bits



Can be in 1 of 2^n states

“Quantum” bit

can be in two possible states,
0 or 1, simultaniously

https://en.wikipedia.org/wiki/Qubit

“Quantum” bit

can be in two possible states,
0 or 1, simultaniously

$$|0\rangle + |1\rangle$$

https://en.wikipedia.org/wiki/Qubit

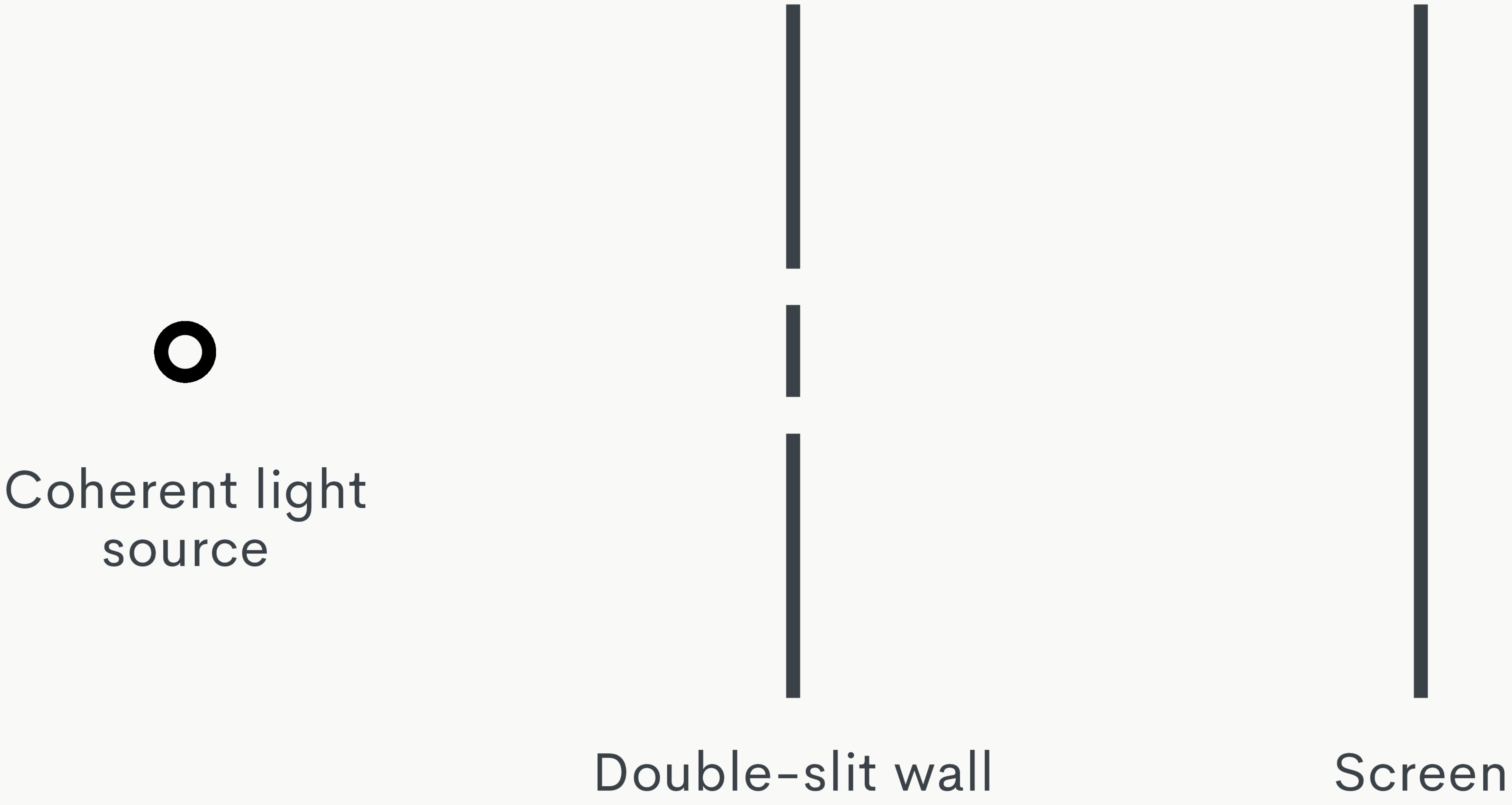
n “quantum” bits

can be in 2^n states simultaneously

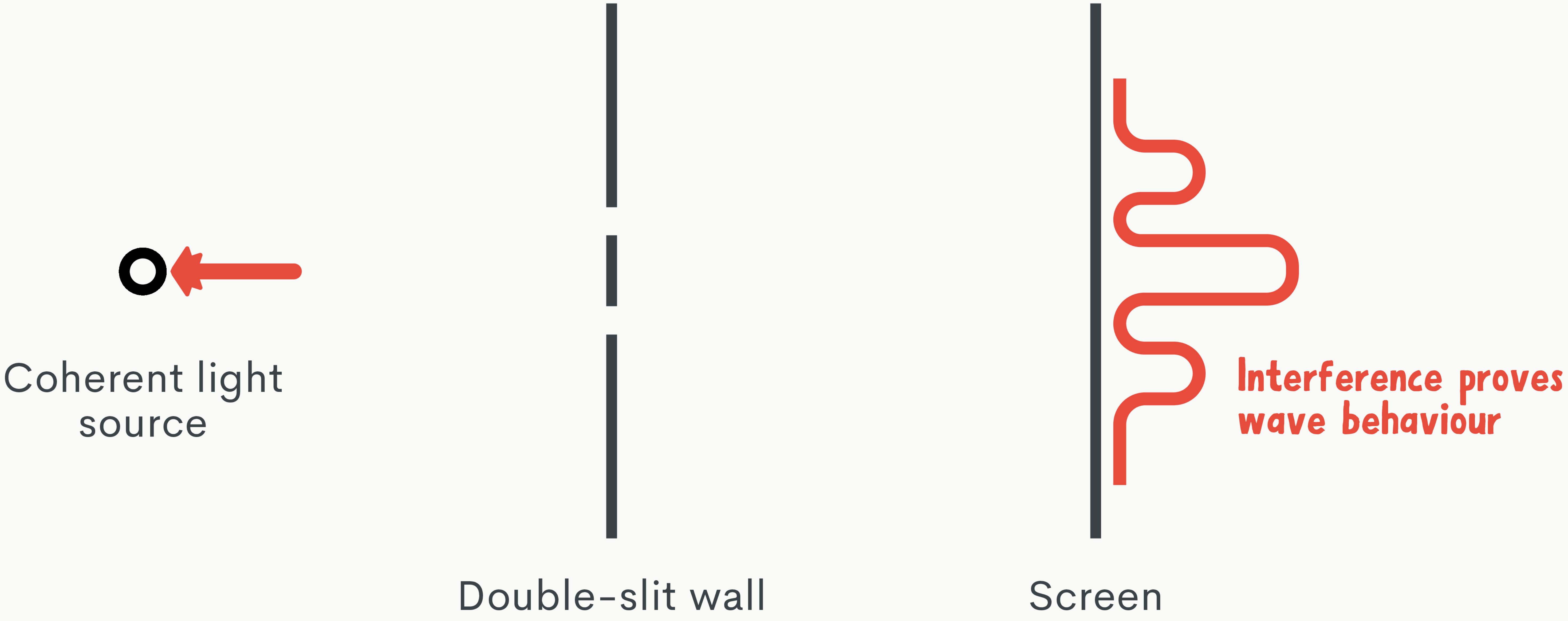
$$|0\rangle + |1\rangle + |2\rangle + \ldots + |2^n\rangle$$

https://en.wikipedia.org/wiki/Qubit

Part I: Quantum computing fundamentals — Superposition & interference

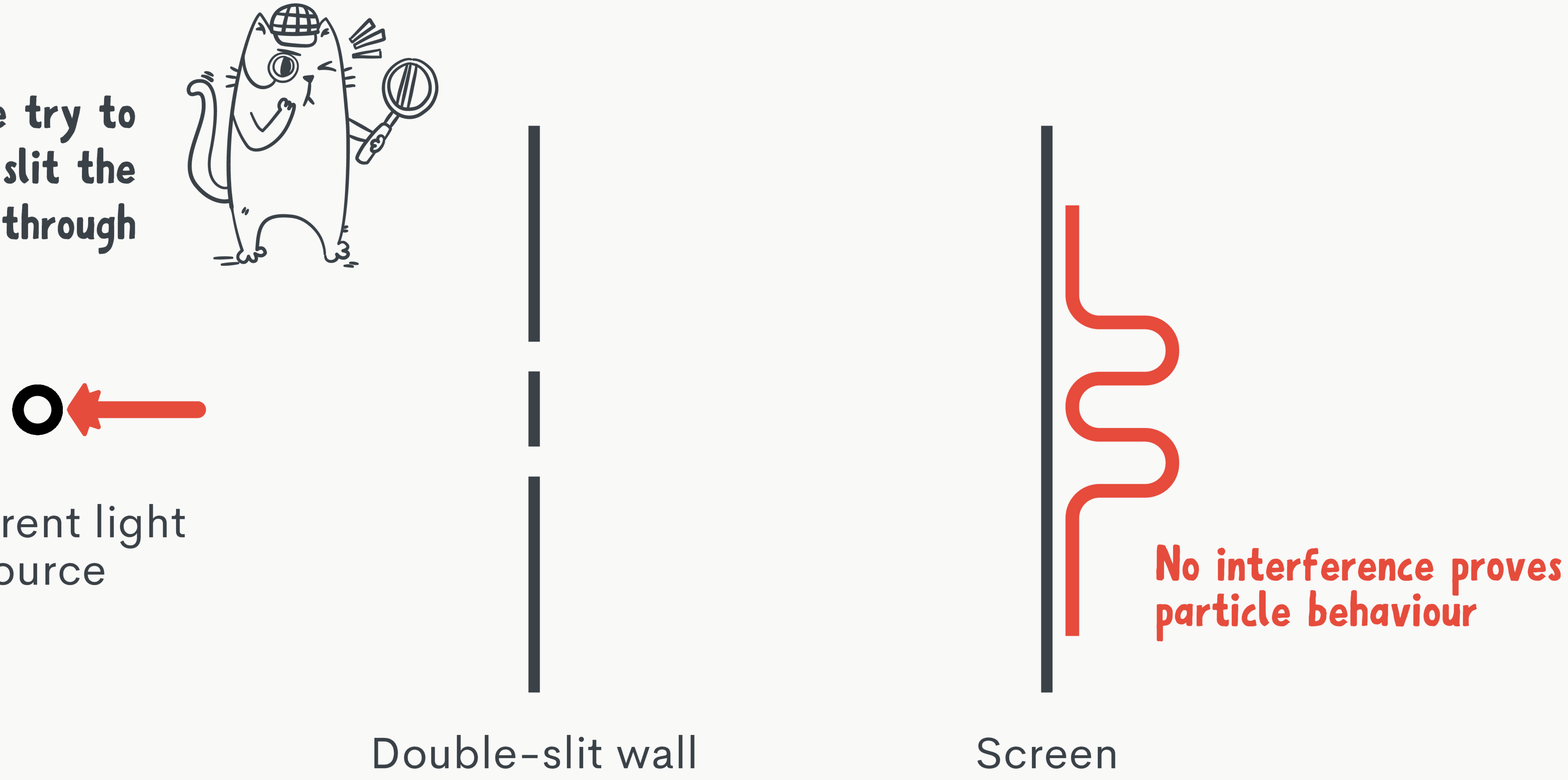


https://en.wikipedia.org/wiki/Double-slit_experiment



https://en.wikipedia.org/wiki/Double-slit_experiment

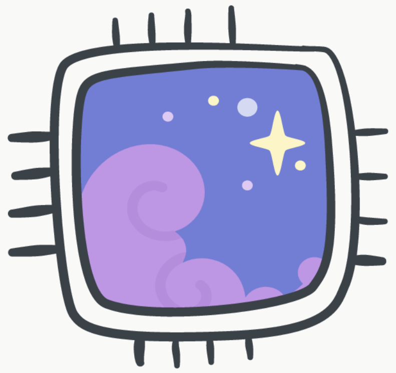
When we try to observe which slit the light goes through



https://en.wikipedia.org/wiki/Double-slit_experiment

Part I: Quantum computing fundamentals — Qubit superposition & interference

$$x + 2 = 3$$



Quantum
circuit

$$x = |0\rangle + |1\rangle + |2\rangle + |3\rangle + \ldots \quad \longrightarrow \quad |0, false\rangle + |1, true\rangle + |2, false\rangle + \ldots$$

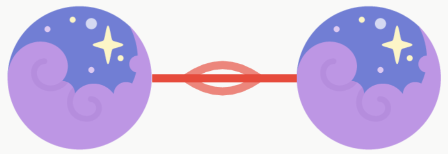
$$|0, false\rangle + |1, true\rangle + |2, false\rangle + \ldots$$

State collapses to a single value when being measured

[redacted] $+$ [redacted] $+ |2, false\rangle +$ [redacted]

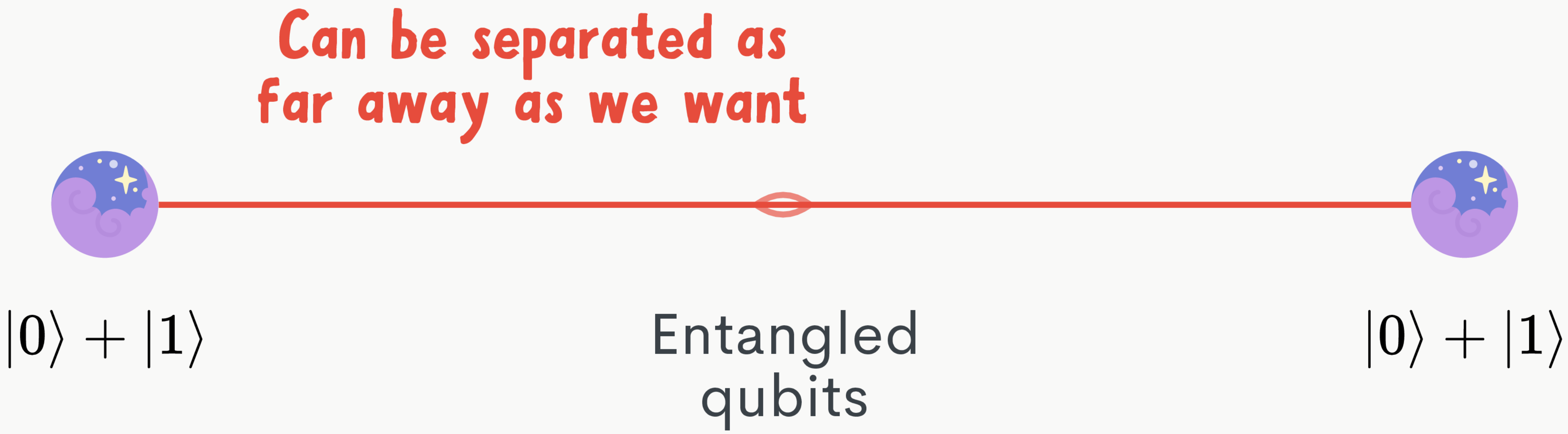
Part I: Quantum computing fundamentals — Entanglement

https://en.wikipedia.org/wiki/Quantum_entanglement



Entangled
qubits

https://en.wikipedia.org/wiki/Quantum_entanglement



https://en.wikipedia.org/wiki/Quantum_entanglement

When we observe one, both collapse so we know the value of both qubits

1

0

https://en.wikipedia.org/wiki/Quantum_entanglement

“Spooky action at a distance”

— Albert Einstein

Letters between Einstein and Max & Hedwig Born — https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.20.8324

Part II: Shor's algorithm breaking RSA encryption

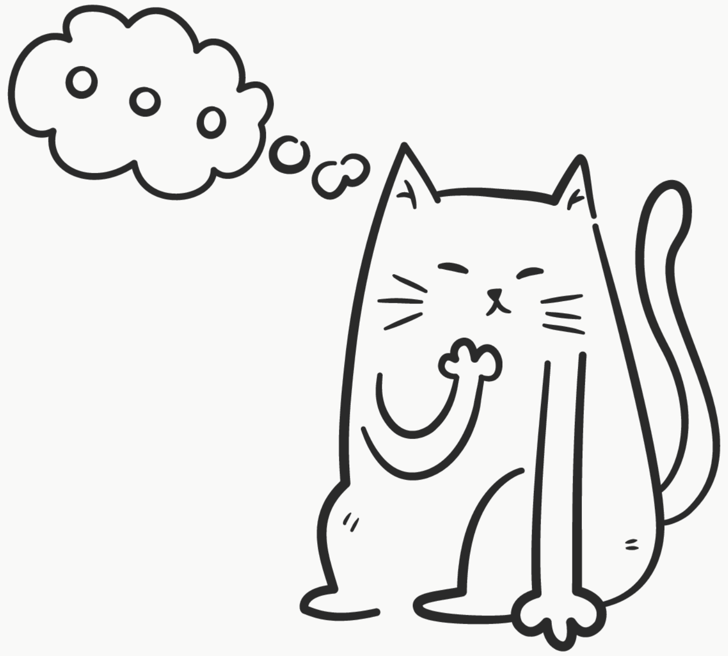
Modern
RSA encryption

$$N = a \times b$$

Modern
RSA encryption

Really large
number

You need its factors to
decrypt the message



$$N = a \times b$$

Modern
RSA encryption

Really large
number

You need its factors to
decrypt the message

https://www.math.rwth-aachen.de/~Greg.Gamble/gap4r3/pkg/factint/htm/CHAP005.htm

Even with supercomputer, guessing by brute force would take over 300 trillion years

$$N = a \times b$$

Modern RSA encryption

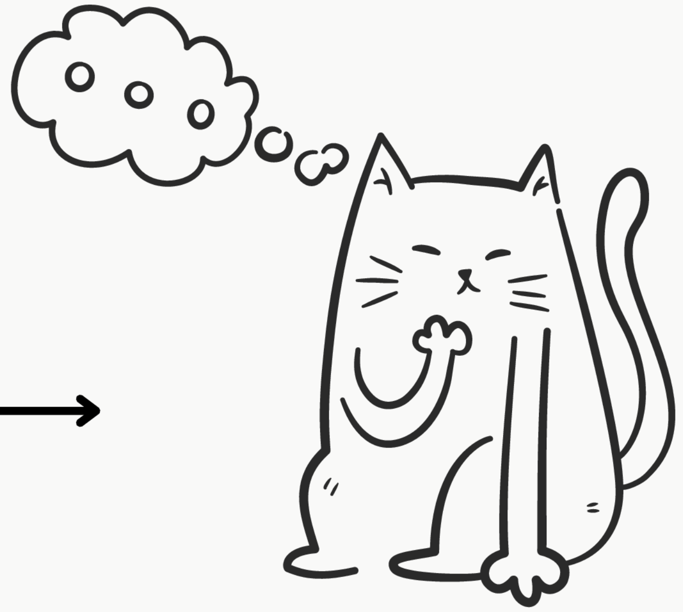
Really large number

You need its factors to decrypt the message

https://www.quintessencelabs.com/blog/breaking-rsa-encryption-update-state-art

Modern
RSA encryption

→

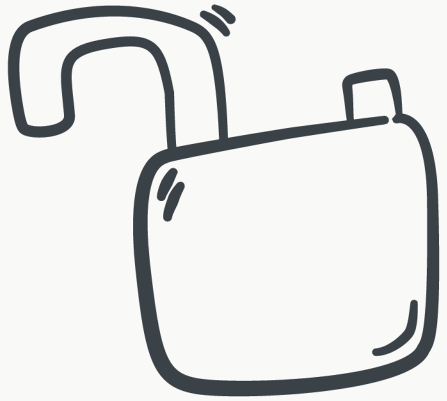


Making a
crappy guess

→

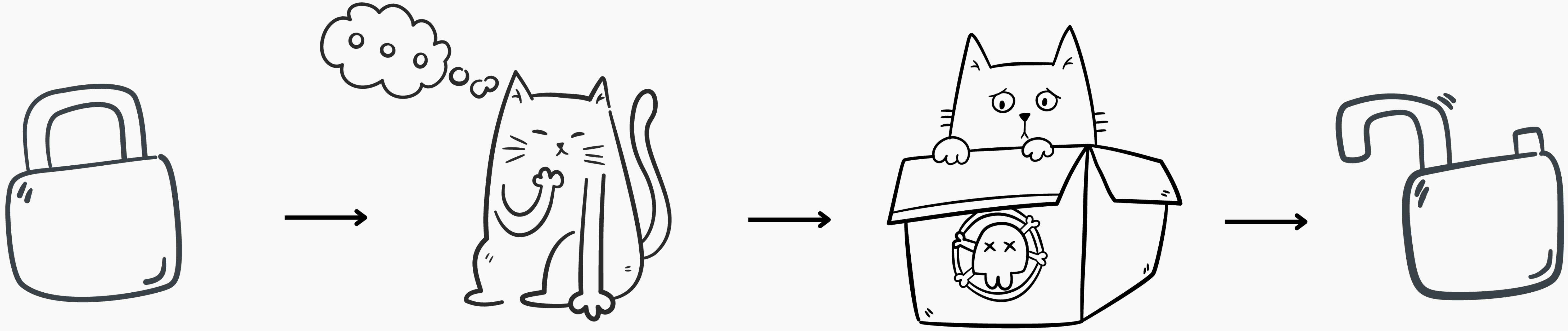
300
trillion
years

→



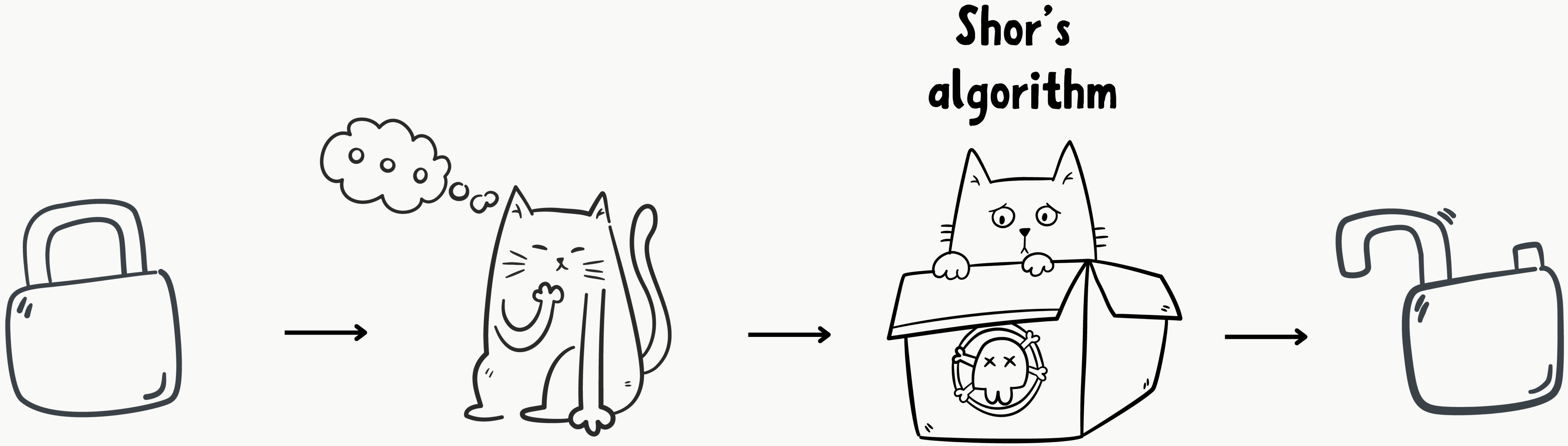
Break
encryption

Part II: Shor's algorithm breaking RSA encryption



Modern RSA encryption → Making a crappy guess → "magic box" turns bad guess into good one → Break encryption

Part II: Shor's algorithm breaking RSA encryption



Modern
RSA encryption

Making a
crappy guess

"magic box"
turns bad
guess into
good one

Break
encryption

$$A \times A \times A \times \ldots \times A = m \times B + 1$$

$$A^p = m \times B + 1$$

https://en.wikipedia.org/wiki/Multiplicative_group_of_integers_modulo_n

$$g^p = m \times N + 1$$

https://en.wikipedia.org/wiki/Multiplicative_group_of_integers_modulo_n

$$g^p = m \times N + 1$$

$$g^p - 1 = m \times N$$

https://en.wikipedia.org/wiki/Multiplicative_group_of_integers_modulo_n

$$g^p = m \times N + 1$$

$$g^p - 1 = m \times N$$

$$(g^{p/2} + 1) \times (g^{p/2} - 1) = m \times N$$

https://en.wikipedia.org/wiki/Multiplicative_group_of_integers_modulo_n

$$g^p = m \times N + 1$$

$$g^p - 1 = m \times N$$

$$(g^{p/2} + 1) \times (g^{p/2} - 1) = m \times N$$

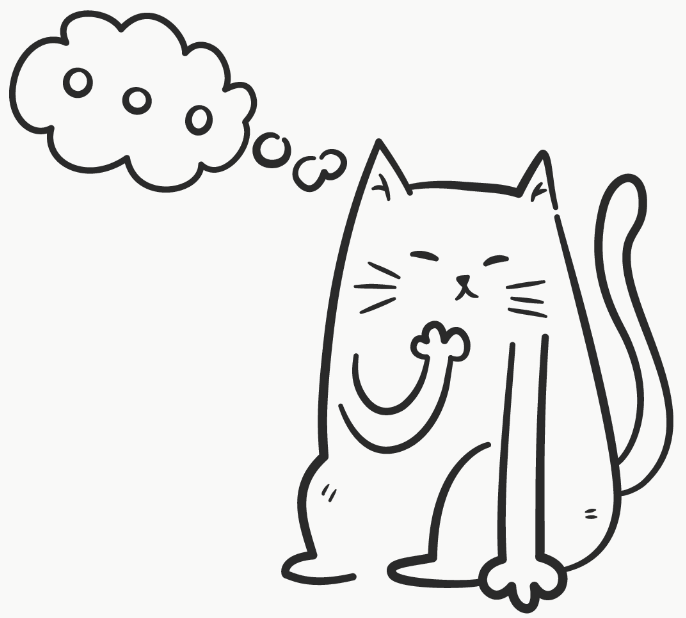
Something

Something else

Shares factors with N

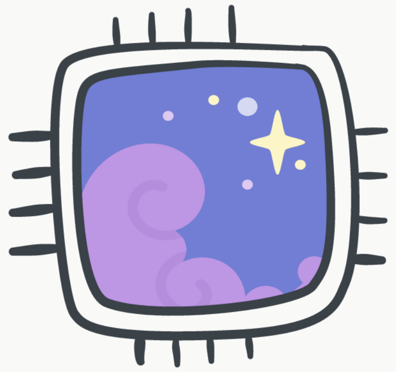
https://en.wikipedia.org/wiki/Multiplicative_group_of_integers_modulo_n

Part II: Shor's algorithm breaking RSA encryption



Making a crappy guess

→



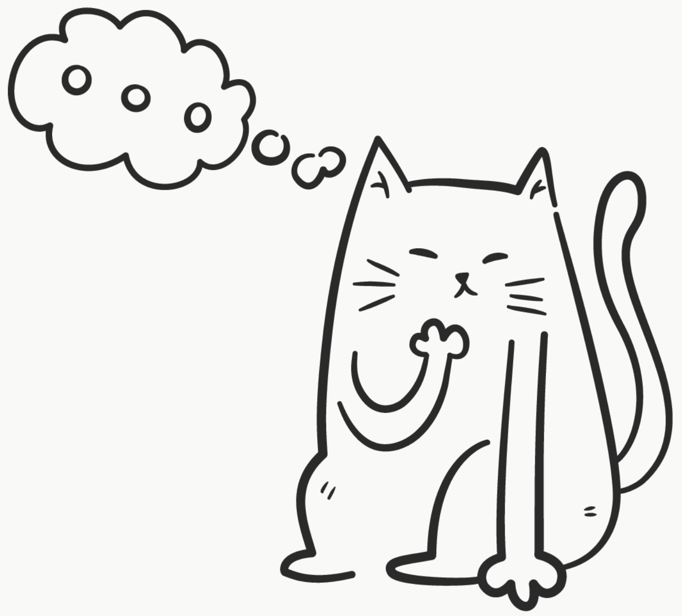
Shor's algorithm turns bad guess into good one

→

◇

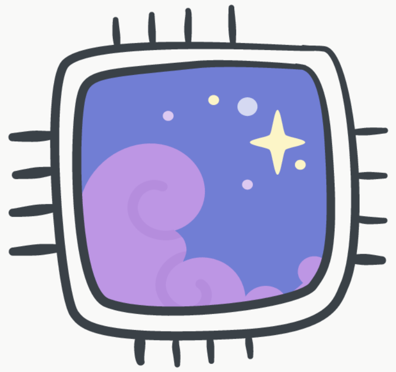
Check for problems

Part II: Shor's algorithm breaking RSA encryption



Making a crappy guess

→



Shor's algorithm turns bad guess into good one

→

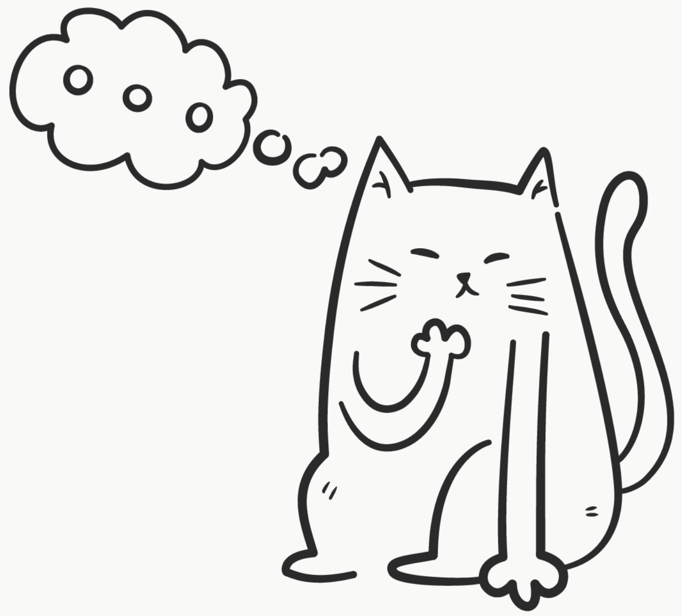
◇

Check for problems

Multiple of N?

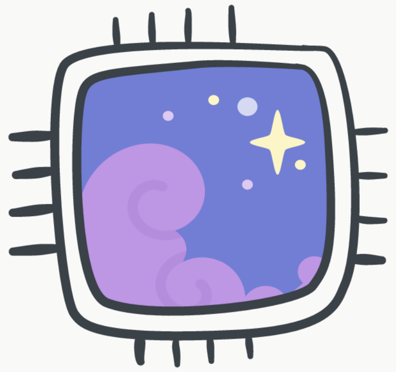
https://www.youtube.com/watch?v=lvTqbM5Dq4Q

Part II: Shor's algorithm breaking RSA encryption



Making a crappy guess

→



Shor's algorithm turns bad guess into good one

→

◇

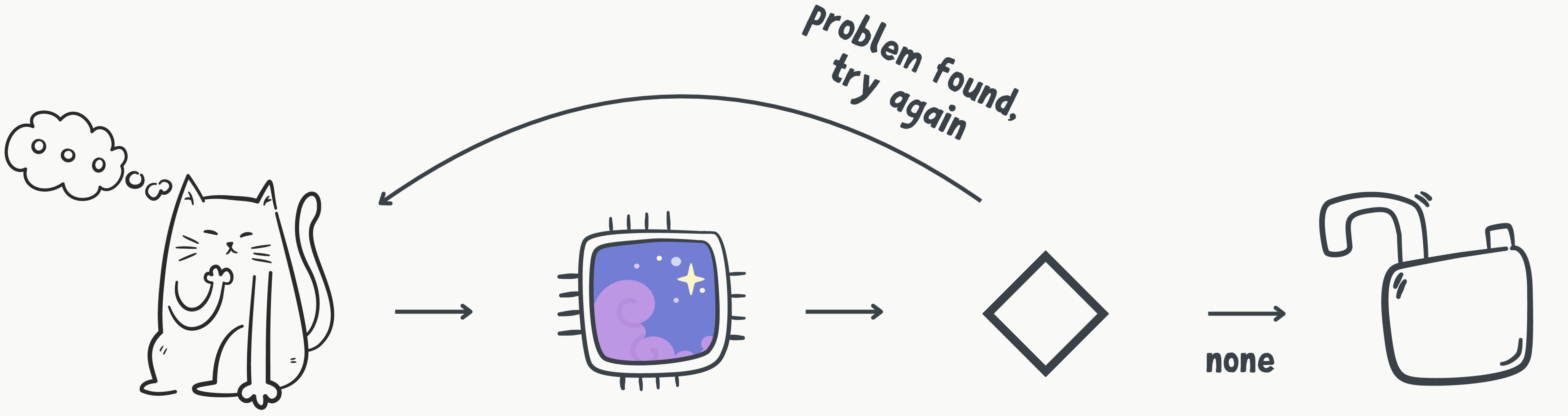
Check for problems

Multiple of N?

Not an integer?

https://www.youtube.com/watch?v=lvTqbM5Dq4Q

Part II: Shor's algorithm breaking RSA encryption



Making a crappy guess

Shor's algorithm turns bad guess into good one

Check for problems

Multiple of N?

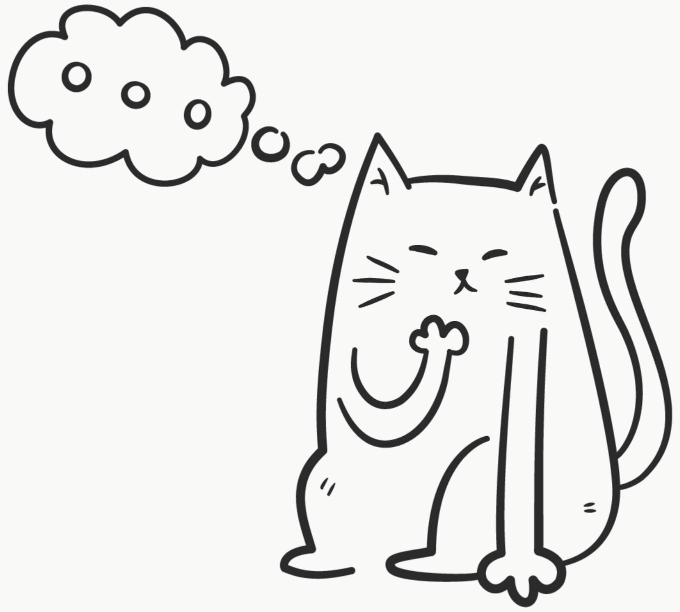
Not an integer?

Break encryption

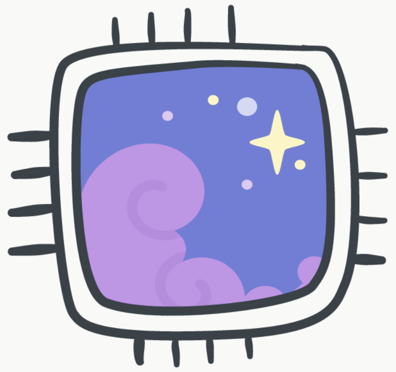
https://www.youtube.com/watch?v=lvTqbM5Dq4Q

99% chance of success in less than 10 tries!

problem found, try again



Making a crappy guess



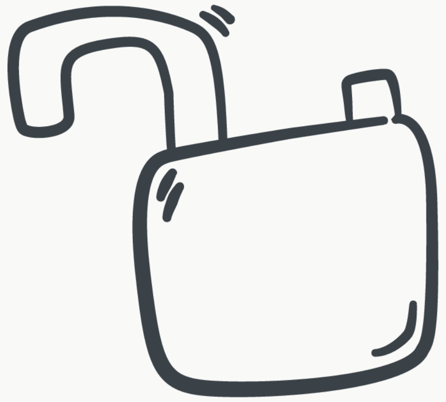
Shor's algorithm turns bad guess into good one

Check for problems

Multiple of N?

Not an integer?

none



Break encryption

https://www.youtube.com/watch?v=lvTqbM5Dq4Q

Part II: Shor's algorithm breaking RSA encryption

https://www.youtube.com/watch?v=lvTqbM5Dq4Q

$$g^p = m \times N + 1$$

$$g^p = 1 \mod N$$

$$g^p = 1 \mod N$$

$$g^x = r \mod N$$

e.g. for x=21, we might get a remainder r=3

$$g^p = 1 \mod N$$

$$g^x = r \mod N$$
$$g^{x+p} = r \mod N$$

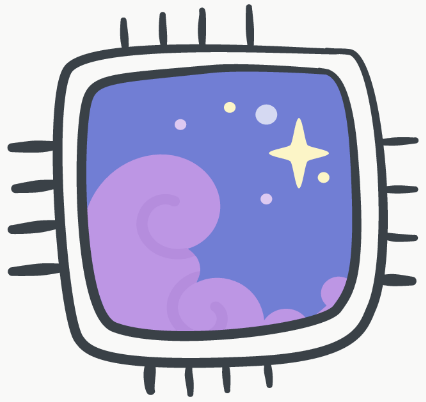
e.g. for x=21, we might get a remainder r=3

$$g^p = 1 \mod N$$

$$g^x = r \mod N$$
$$g^{x+p} = r \mod N$$
$$g^{x+2p} = r \mod N$$

e.g. for x=21, we might
get a remainder r=3

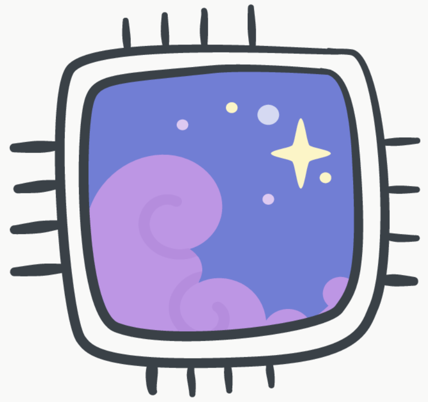
$$g^x = r \mod N$$



Quantum circuit

$\longrightarrow$

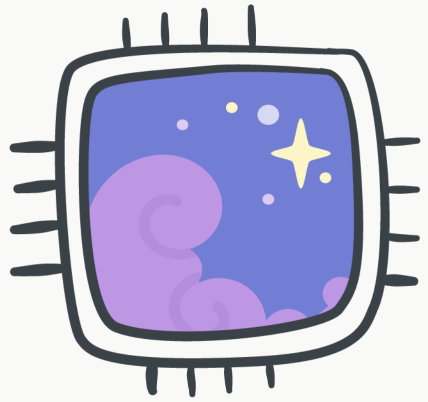
$$g^x = r \mod N$$



Quantum circuit

$$x = |0\rangle + |1\rangle + |2\rangle + \dots \longrightarrow$$

$$g^x = r \mod N$$



Quantum circuit

$$x = |0\rangle + |1\rangle + |2\rangle + \dots \quad \longrightarrow \quad |0, +17\rangle + |1, +3\rangle + |2, +92\rangle + \dots$$

$$|\mathbf{0}, +\mathbf{17}\rangle + |\mathbf{1}, +\mathbf{3}\rangle + |\mathbf{2}, +\mathbf{92}\rangle + \ldots$$

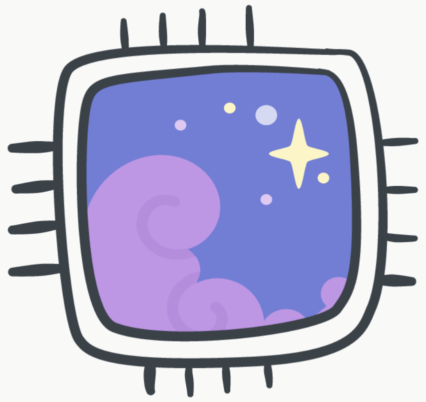
only measure the remainder value

$$|1, +3\rangle + |11, +3\rangle + |21, +3\rangle + \ldots$$

only measure the
remainder value

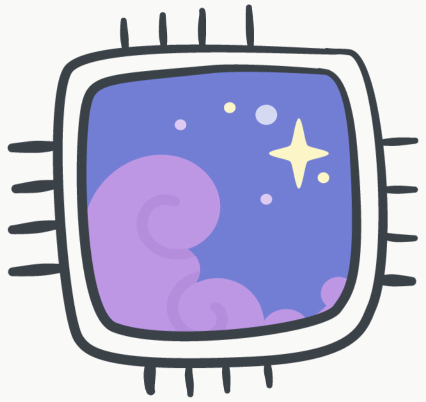
$$|1\rangle + |11\rangle + |21\rangle + |31\rangle + |41\rangle + \ldots$$

the resulting superposition will
have a frequency of 1 over p



Quantum Fourier Transform

https://www.youtube.com/watch?v=lvTqbM5Dq4Q

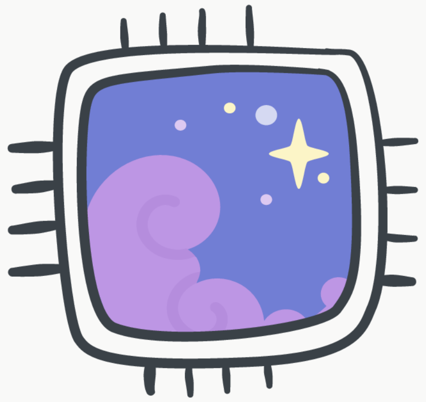


Quantum
Fourier
Transform

$$|1\rangle + |11\rangle + |21\rangle + |31\rangle + \ldots \longrightarrow 1 \div 10$$

the result is the frequency of the superposition

Part II: Shor's algorithm breaking RSA encryption

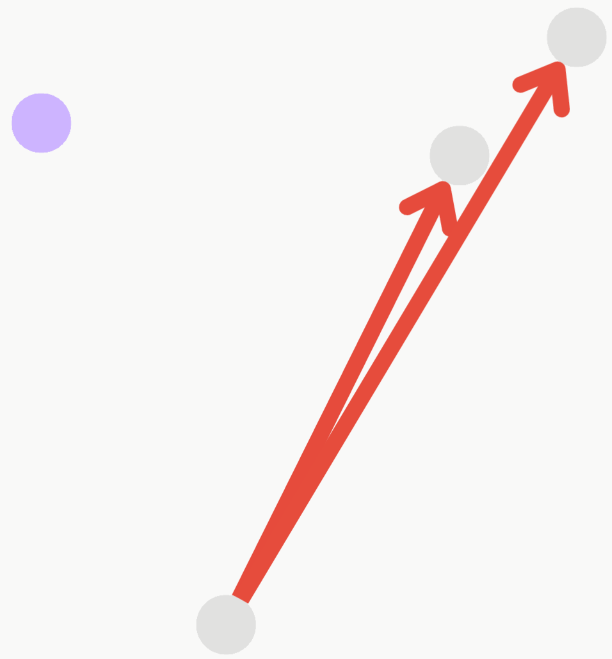


QPU: modulo calculation + QFT

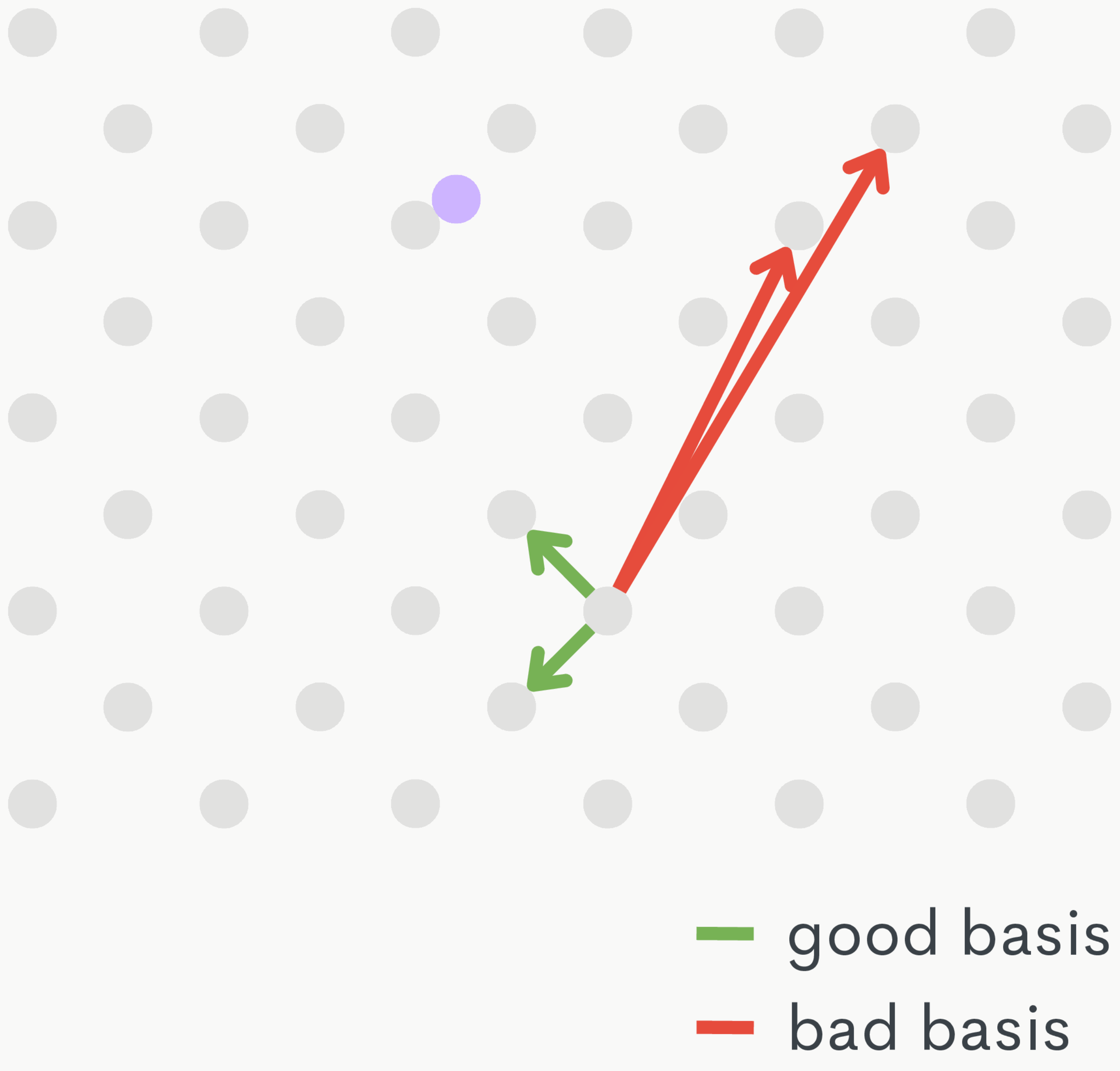
"Classical" Computer

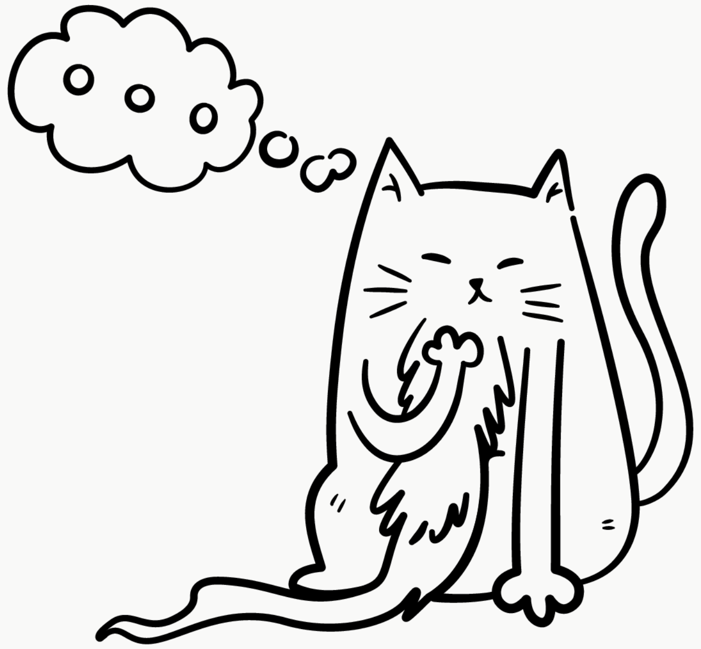
Part II: Shor's algorithm breaking RSA encryption — Post quantum cryptography

Which combination of vectors is closest to the given point?



https://cloud.google.com/blog/products/identity-security/why-google-now-uses-post-quantum-cryptography-for-internal-comms





finding the closest point with vectors of the bad basis in higher dimensions is really hard

https://www.youtube.com/watch?v=QDdOoYdb748

Part II: Shor's algorithm breaking RSA encryption — Current challenges with QPUs

Problem 1: Number of qubits

E.g. to run Shor's algorithm on RSA-2048, you would need around 4,000 logical qubits to have sufficient memory

https://quantum-journal.org/papers/q-2021-04-15-433/

https://en.wikipedia.org/wiki/List_of_quantum_processors

Problem 1: Number of qubits

E.g. to run Shor's algorithm on RSA-2048, you would need around 4,000 logical qubits to have sufficient memory

Problem 2: Error correction

It is really hard to prevent any unintentional outside influence that would cause the quantum state irrevertably to collapse

Problem 1: Number of qubits

E.g. to run Shor's algorithm on RSA-2048, you would need around ~~4,000 logical qubits~~ 2 million physical qubits to have sufficient memory

Problem 2: Error correction

It is really hard to prevent any unintentional outside influence that would cause the quantum state irrevertably to collapse

Part III: Practical applications of quantum computing

Quantum Machine Learning (QML)

Quantum Machine Learning (QML)

- Quantum Fourier Transforms

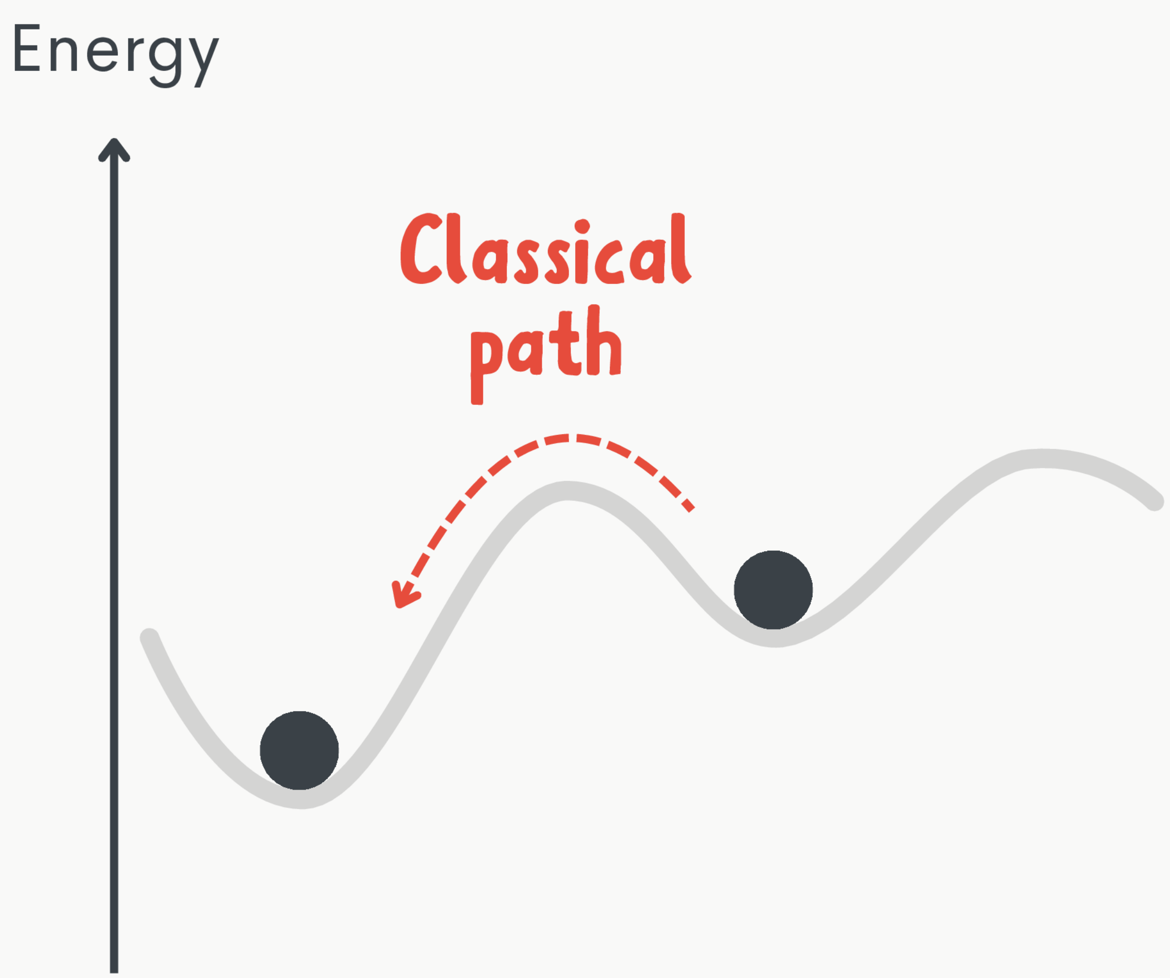
Quantum Machine Learning (QML)

- Quantum Fourier Transforms
- Grover's algorithm

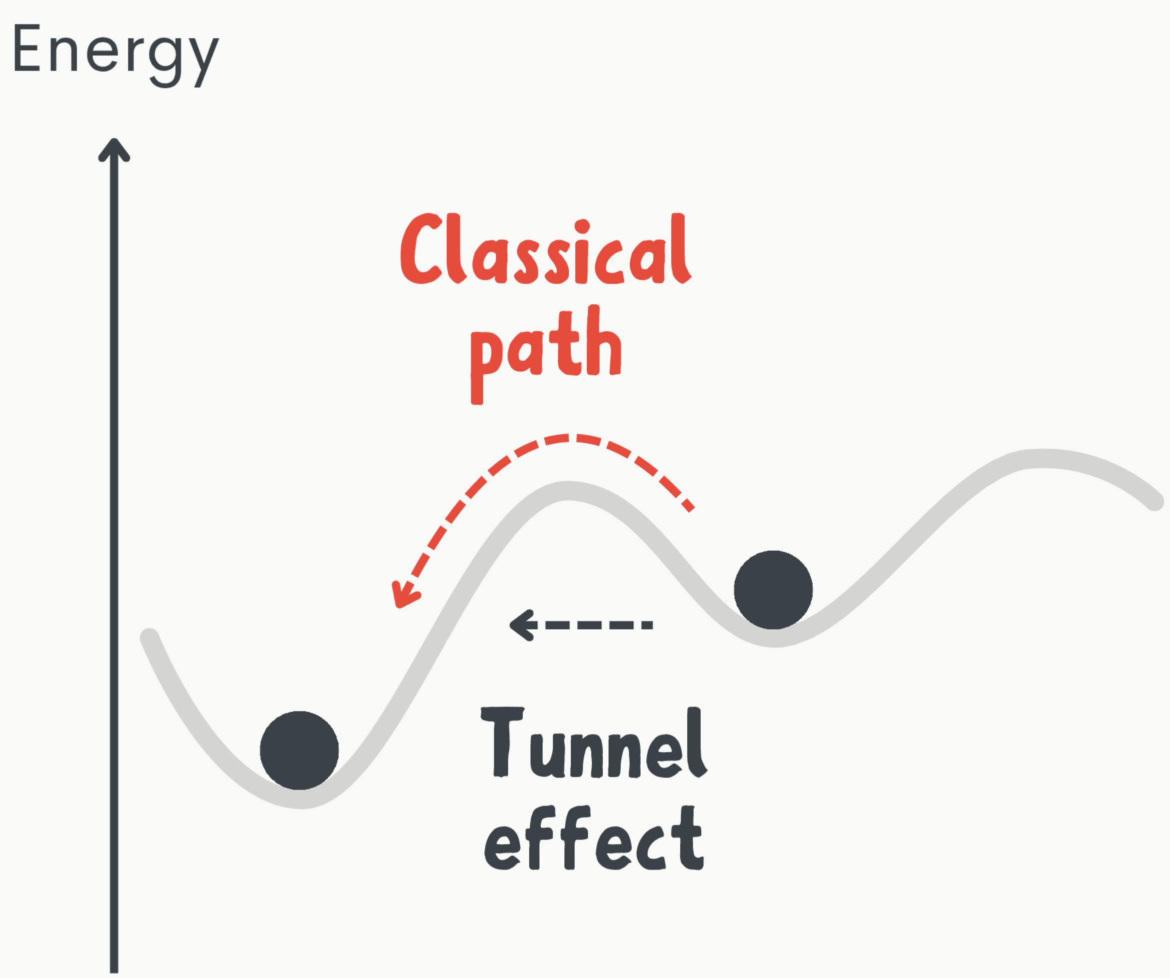
Quantum Machine Learning (QML)

- Quantum Fourier Transforms
- Grover's algorithm
- Quantum annealing

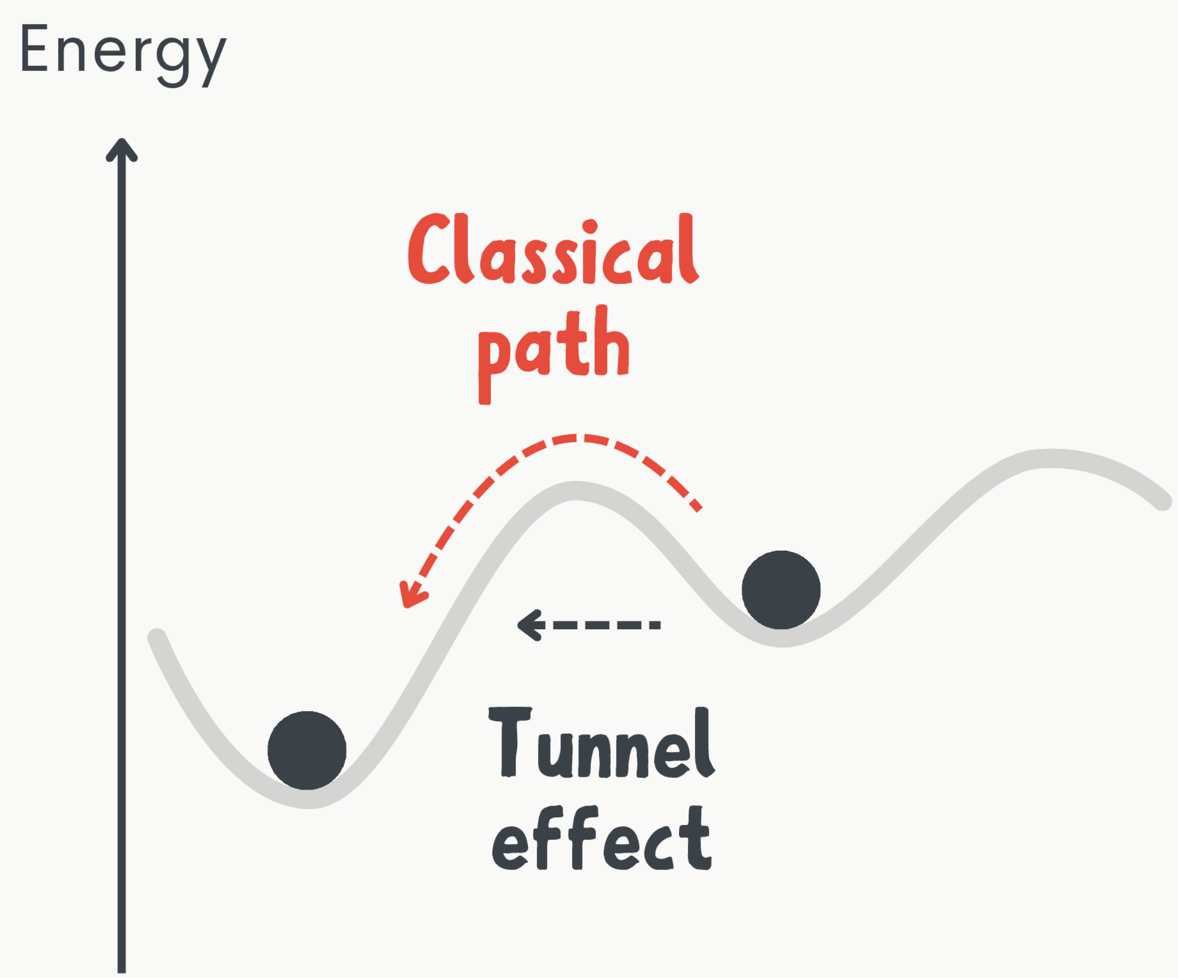
https://medium.com/@quantum_wa/quantum-annealing-cdb129e96601



https://medium.com/@quantum_wa/quantum-annealing-cdb129e96601



https://medium.com/@quantum_wa/quantum-annealing-cdb129e96601



This can cause “vacuum decay” and destroy the whole universe

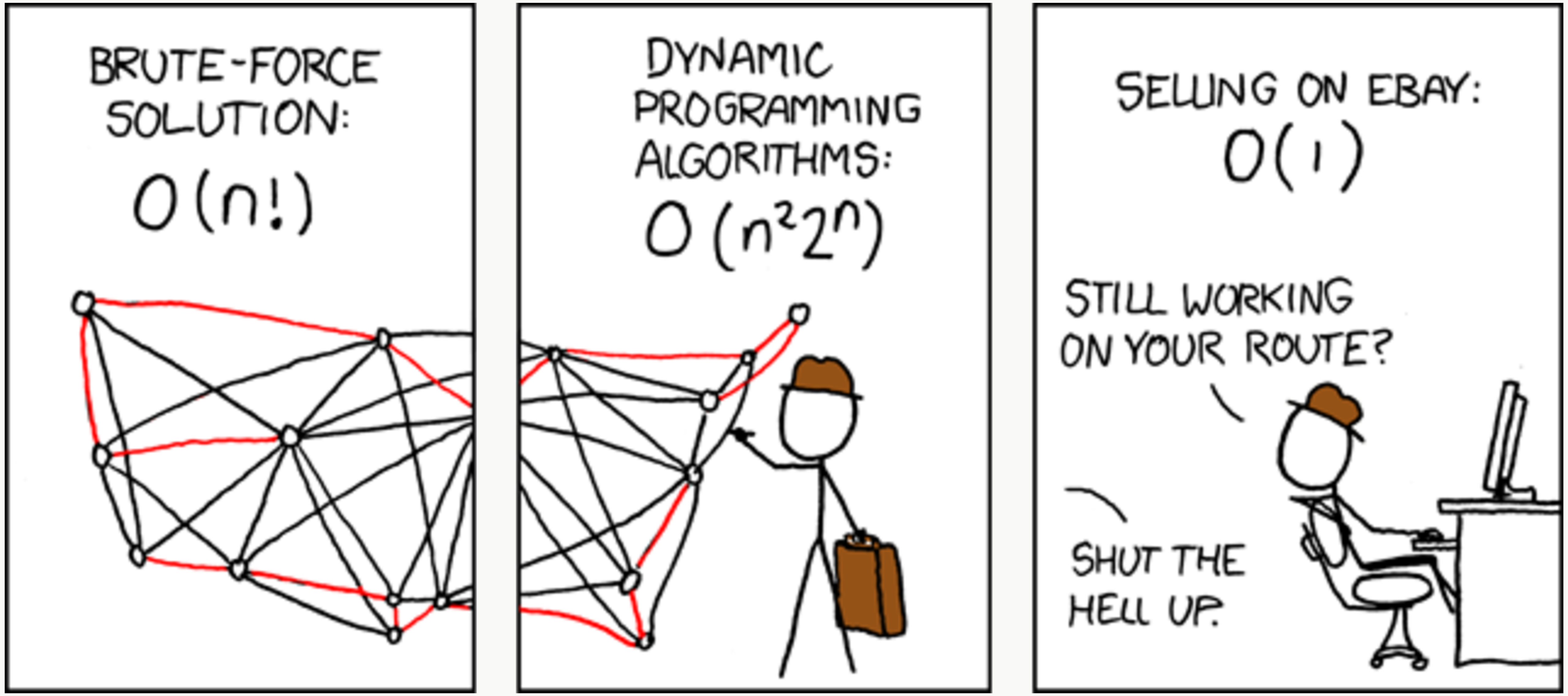
Quantum Machine Learning (QML)

- Quantum Fourier Transforms
- Grover's algorithm
- Quantum annealing

Quantum Simulations

Quantum Simulations

- Optimisation problems



https://xkcd.com/399/

Quantum Simulations

- Optimisation problems

Quantum Simulations

- Optimisation problems
  - Supply chain management

Quantum Simulations

- Optimisation problems
    - Supply chain management
    - Financial modelling and portfolio optimisations

Quantum Simulations

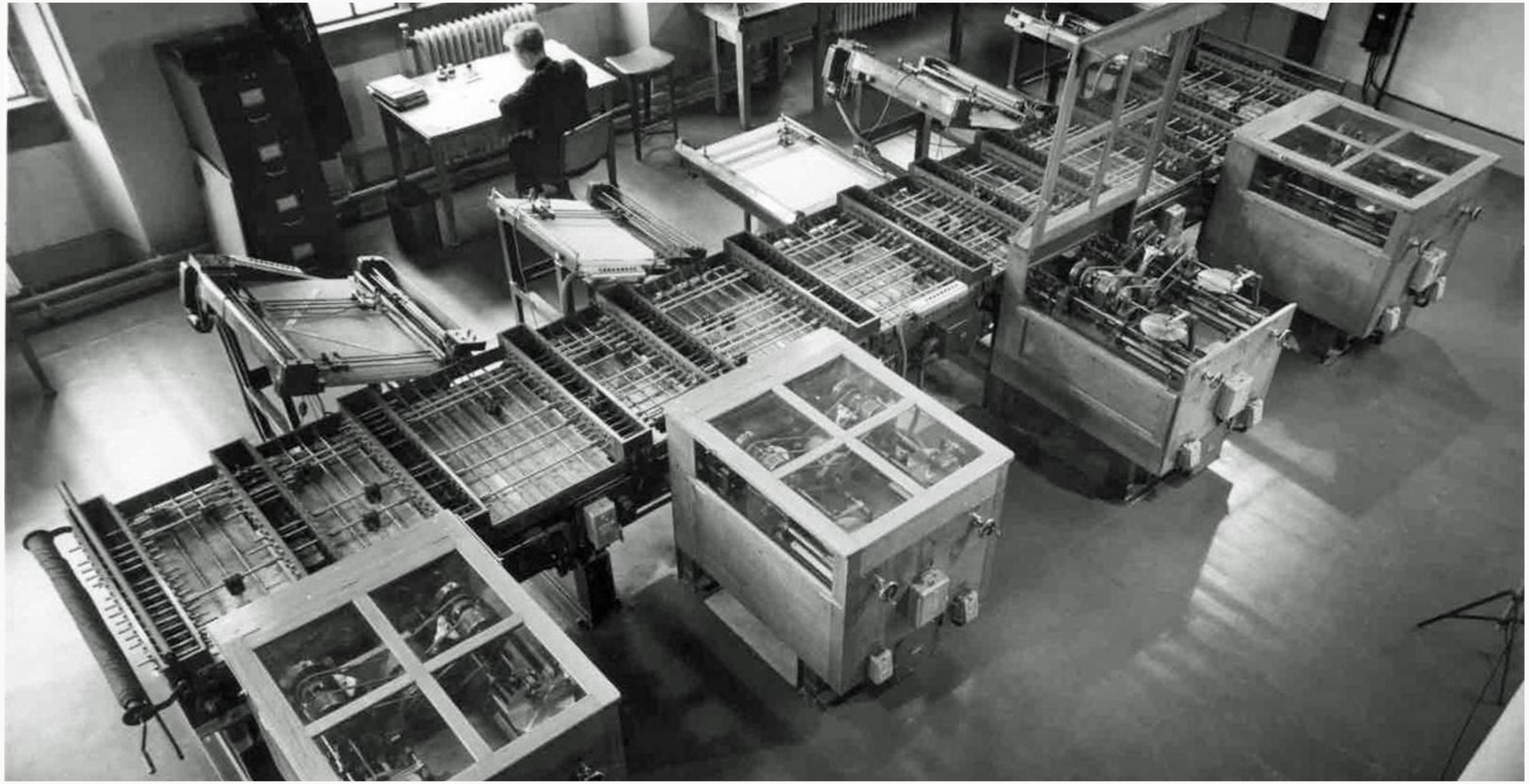
- Optimisation problems
    - Supply chain management
    - Financial modelling and portfolio optimisations
    - Traffic and fleet management optimisations

Quantum Simulations

- Optimisation problems
- Simulating quantum sytems

"Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical."

— Richard Feynman



https://pbs.twimg.com/media/EfCFix5UcAASXVz.jpg

http://amg.nzfmm.co.nz/differential_analyser_explained.html

Quantum Simulations

- Optimisation problems
- Simulating quantum sytems

Quantum Simulations

- Optimisation problems
- Simulating quantum sytems
    - Weather simulations and forecasting

Quantum Simulations

- Optimisation problems
- Simulating quantum sytems
    - Weather simulations and forecasting
    - Drug manufacturing & protein folding

Conclusion

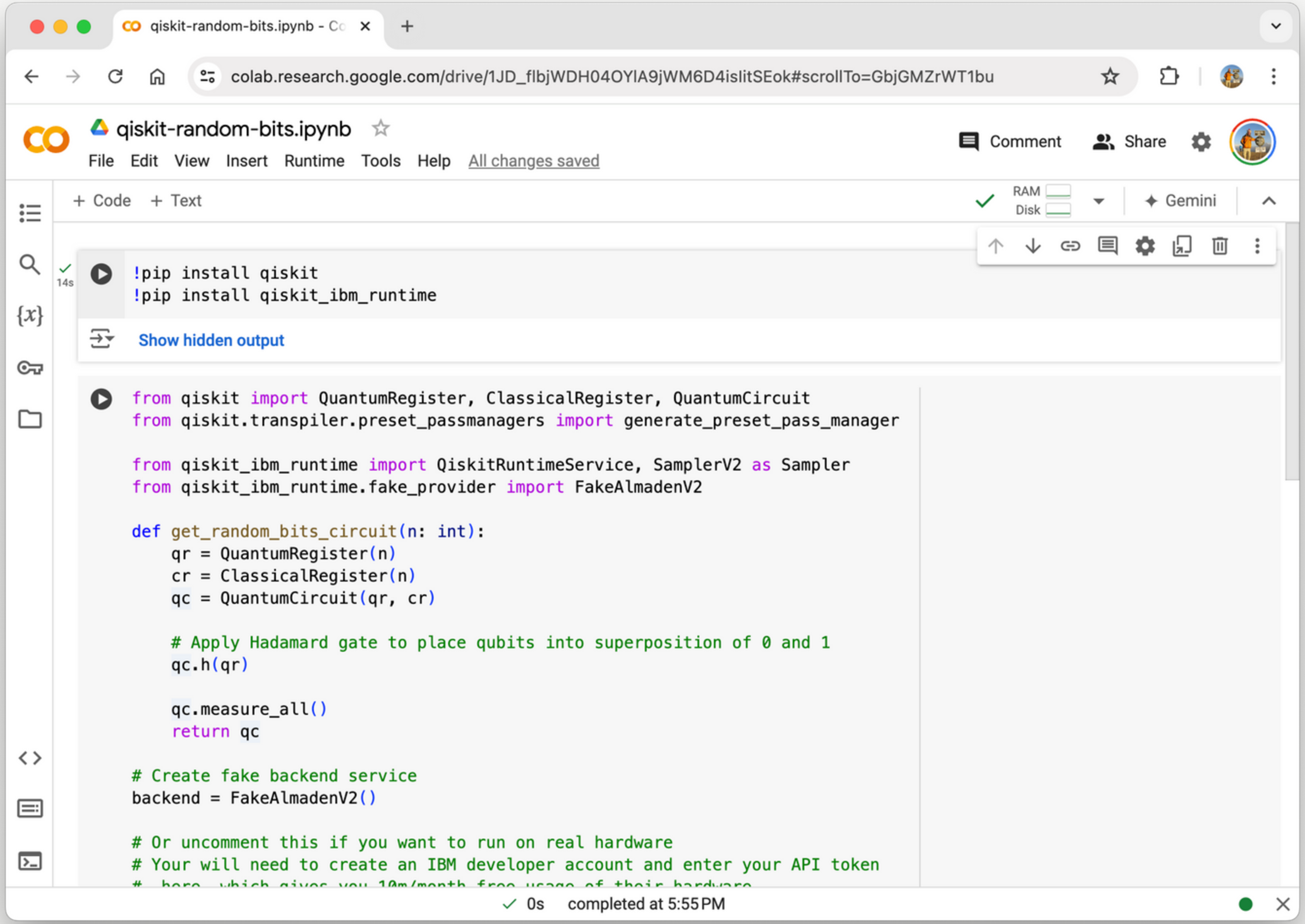
Qiskit – IBM quantum computing development kit

https://docs.quantum.ibm.com/start

https://github.com/Qiskit

https://www.youtube.com/@qiskit

Conclusion — Using quantum computing today



Let's you run quantum circuits in simulators and against real hardware

https://colab.research.google.com/drive/1JD_flbjWDH04OYlA9jWM6D4islitSEok?usp=sharing

Recommended reading & watching

Programming Quantum Computers by Eric R. Johnson, Nic Harrigan & Mercedes Gimeno-Segovia (O'Reilly)

Youtube video: The Map of Quantum Computing - Quantum Computing Explained

https://www.youtube.com/watch?v=-UlxHPIEVqA, https://dominicwalliman.com/

Youtube channel: IBM Technology

https://www.youtube.com/@IBMTechnology/search?query=quantum

Conclusion — Thank you

Link to the slides:

https://www.julianburr.de/ddd-brisbane-2024-slides.pdf

https://www.linkedin.com/in/julianburr/

https://twitter.com/jburr90

{ } NDC Conferences

RISBANE

Leave feedback to enter the prize draw

Please give me feedback!