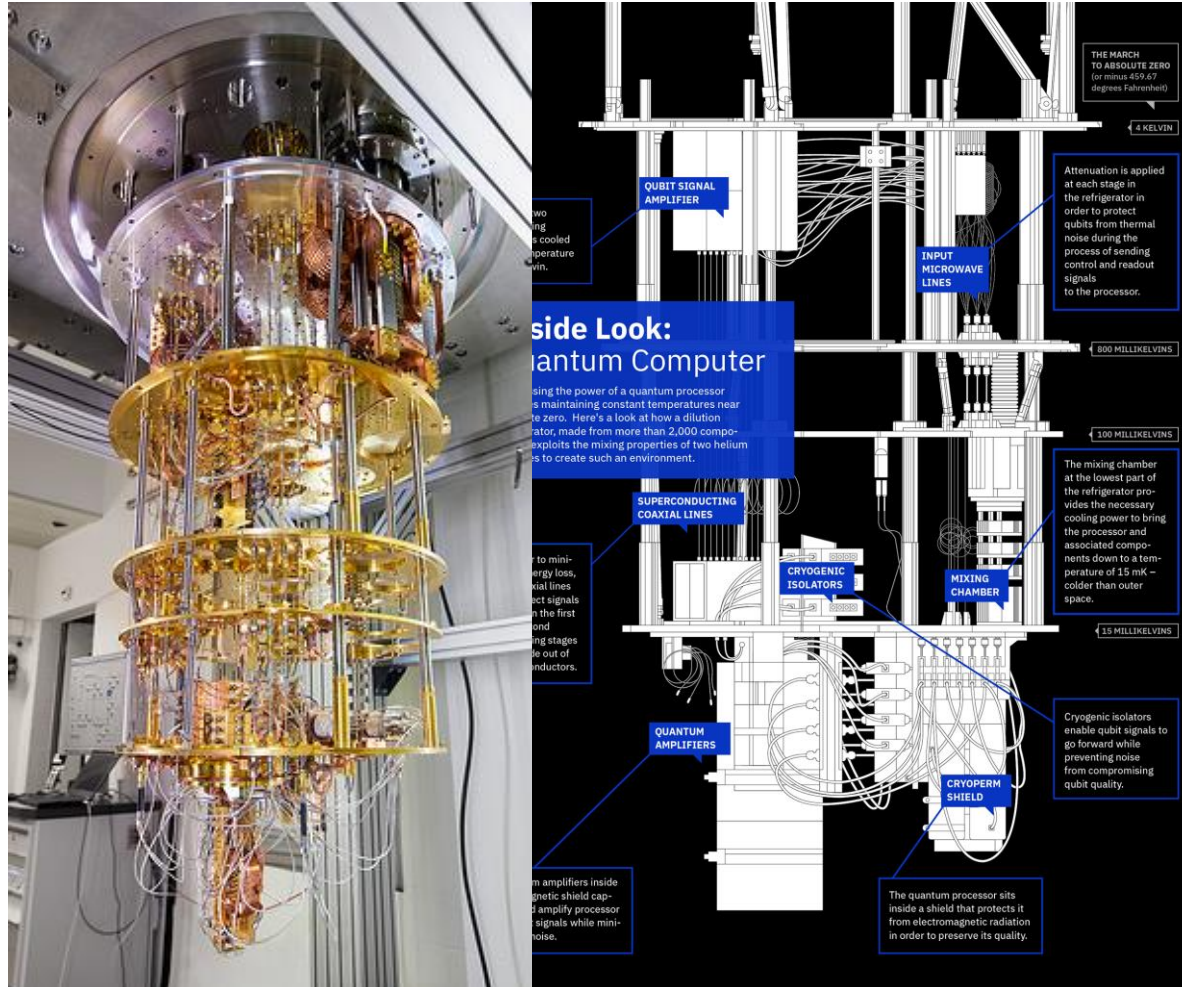


# Quantum Computing

# Outline

- What is a quantum computer like?
- How does quantum computing work?
- Possibilities of quantum computing
- The realization of quantum Fourier transform

# What is a Quantum Computer Like



Companies:

Google 72-qubit

50-qubit



D-Wave

rigetti



IBM's quantum computer

Picture from: <https://www.ibm.com/blogs/research/2018/01/quantum-prizes/>

# How Does Quantum Computing Work

Classical computing fundamental unit: **bit**



On: 1



Off: 0

Quantum computing fundamental unit: **qubit (quatum bit)**



On:  $|1\rangle$



Off:  $|0\rangle$



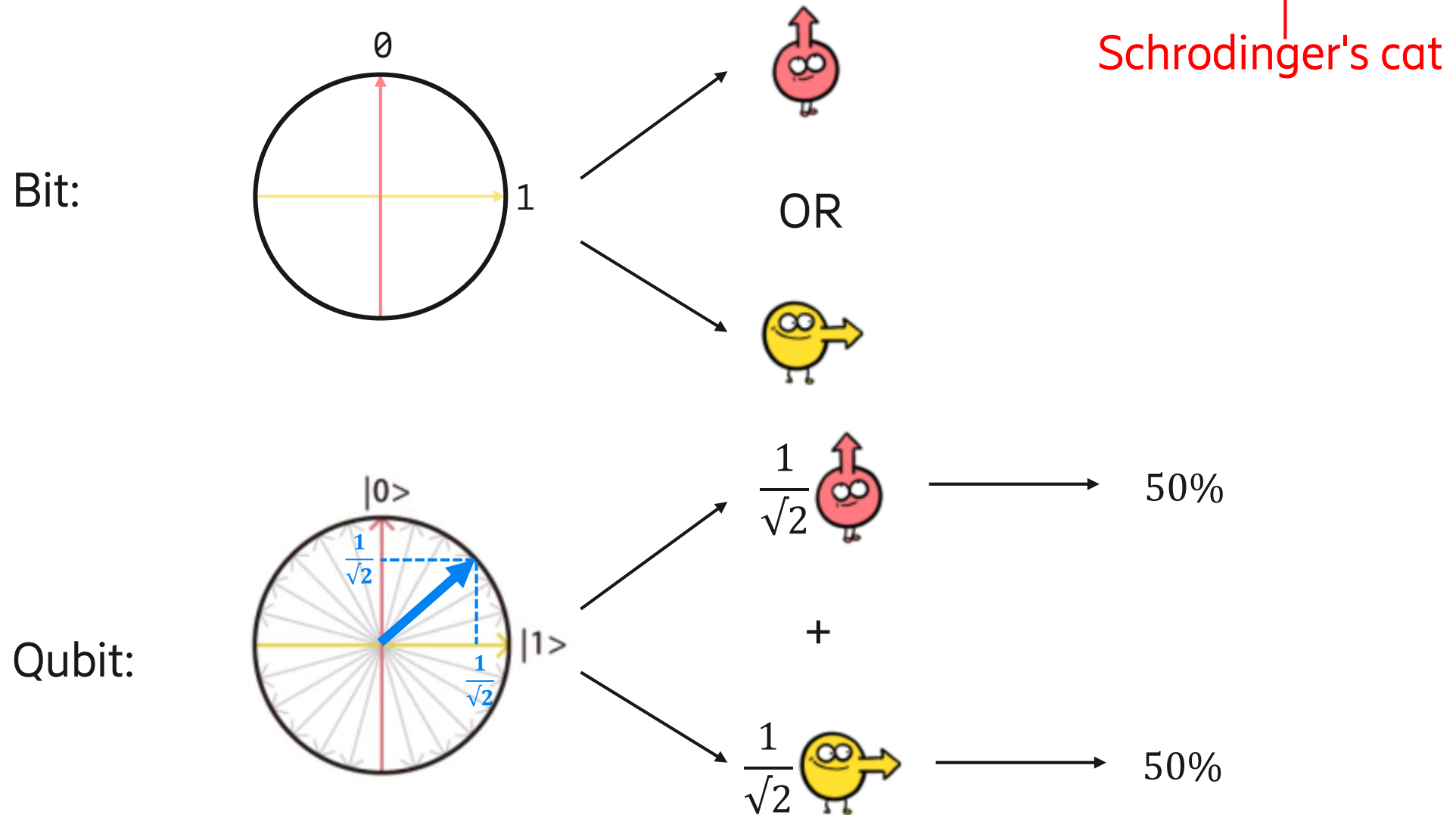
Both:  $\alpha|1\rangle + \beta|0\rangle$

photon

nucleus

electron

# How Does Quantum Computing Work: Superposition



# How Does Quantum Computing Work: Example

2 classical bits:

bit 1	bit 2
0	0
0	1
1	0
1	1

2 qubits:

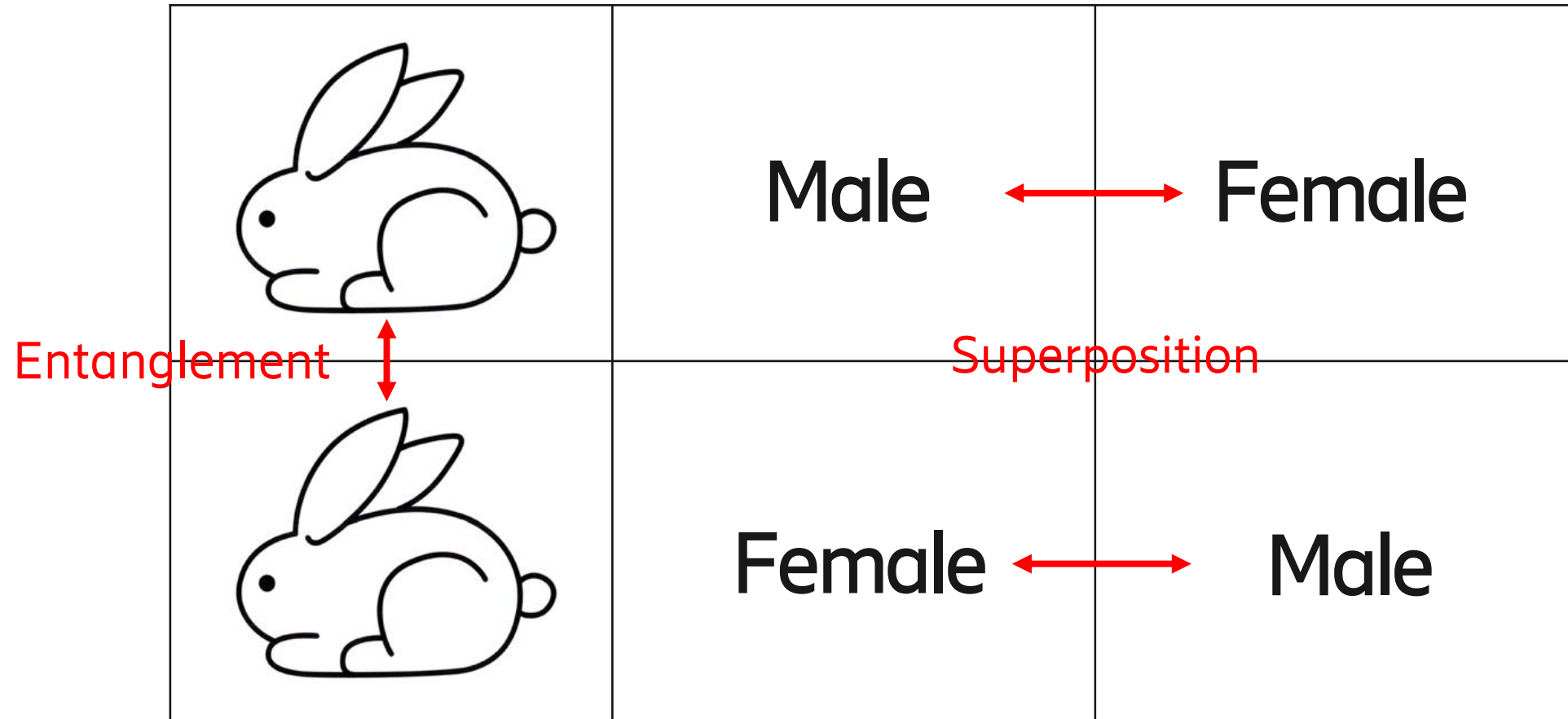
		qubit 1	qubit 2
$\alpha$		0	0
$\beta$		0	1
$\gamma$		1	0
$\delta$		1	1

**2 qubits contain 4 bits of information.**

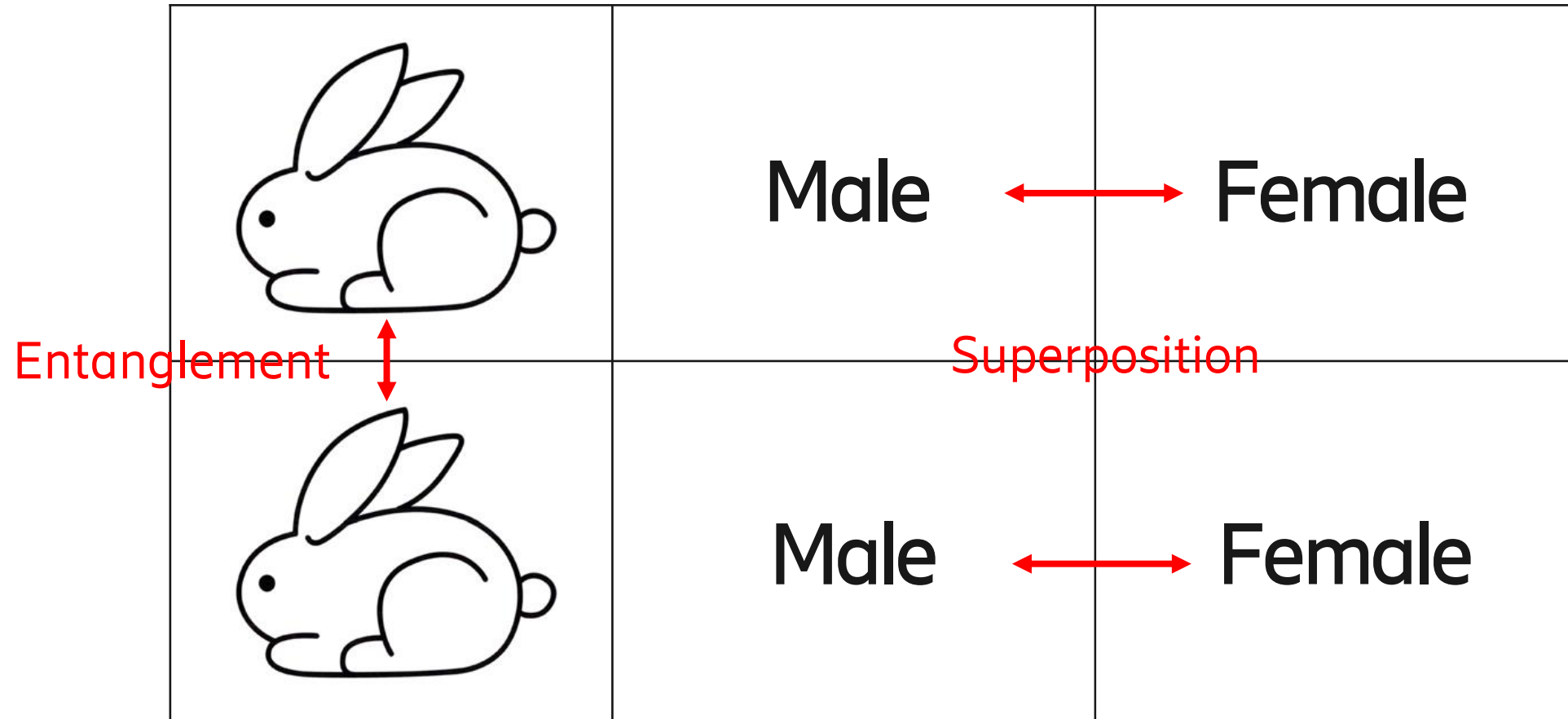
**$N$  qubits contain  $2^N$  bits of information.**

300 qubits  $\rightarrow$  ~2,000,000,000,000,000,000,000,000,000, bits  
000,000,000,000,000,000,000,000,000,  
000,000,000,000,000,000,000,000,000,  
000,000,000,000,000,000,000

# How Does Quantum Computing Work: Entanglement



# How Does Quantum Computing Work: Entanglement

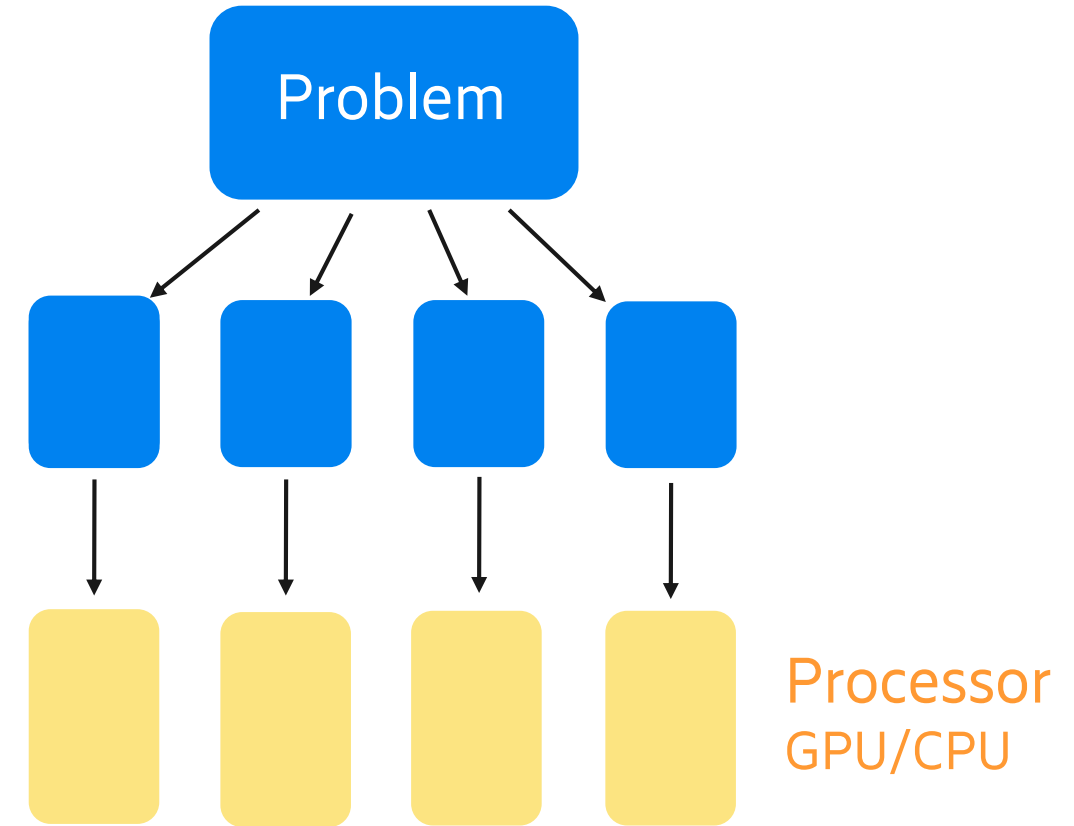
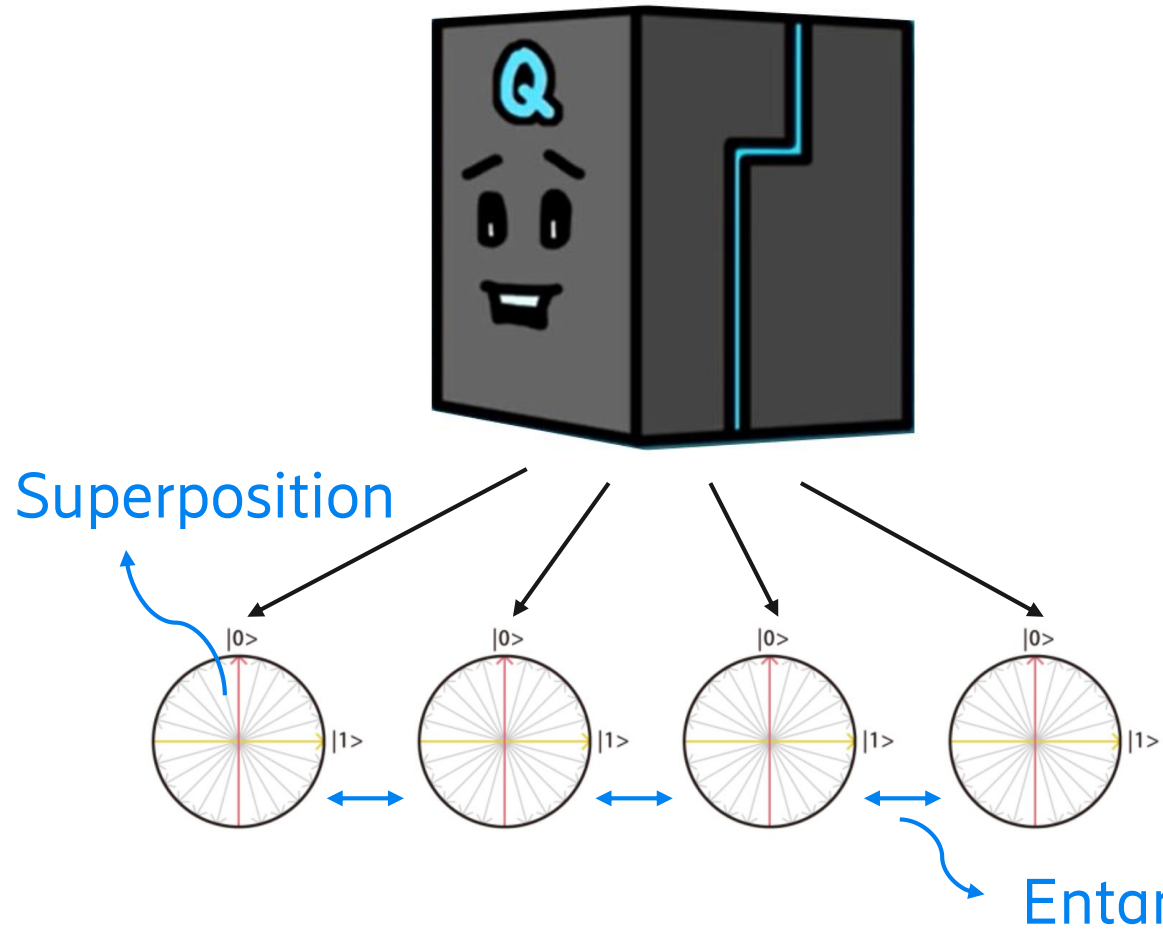




# How Does Quantum Computing Work

Quantum computer

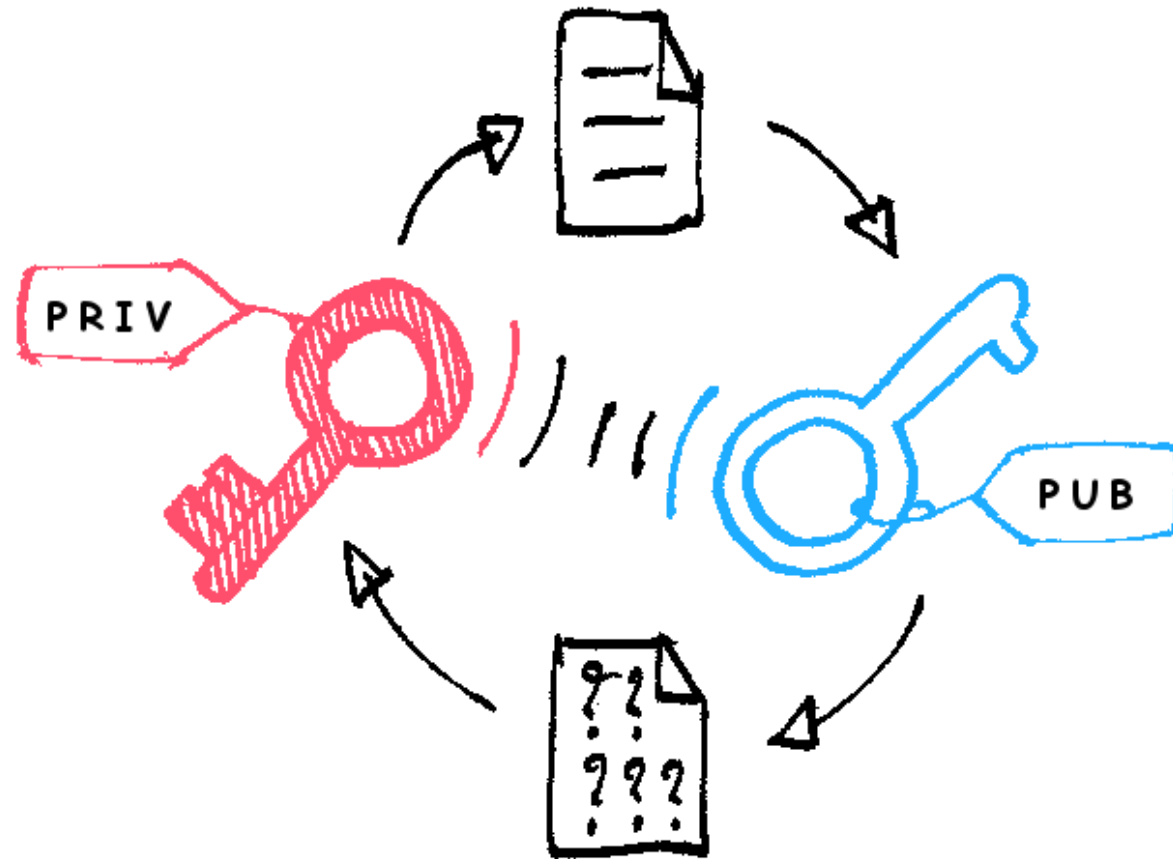
Parallel computer ?



# How Does Quantum Computing Work

	Quantum computer	Parallel computer
1. Entanglement	Entanglement between qubits	Independent processor without entanglement
2. Measurement	One state after measurement	Measure any processors at any time
3. Computational power	<b>Exponentially</b> increase ( $N = 2^n$ )	<b>Linearly</b> increase

# Possibilities of Quantum Computing: Cryptography



Picture from: [https://en.wikipedia.org/wiki/Public-key\\_cryptography](https://en.wikipedia.org/wiki/Public-key_cryptography)

# Possibilities of Quantum Computing: Cryptography

Parallel computing → Large compute power

RSA Algorithm: large integer factorization

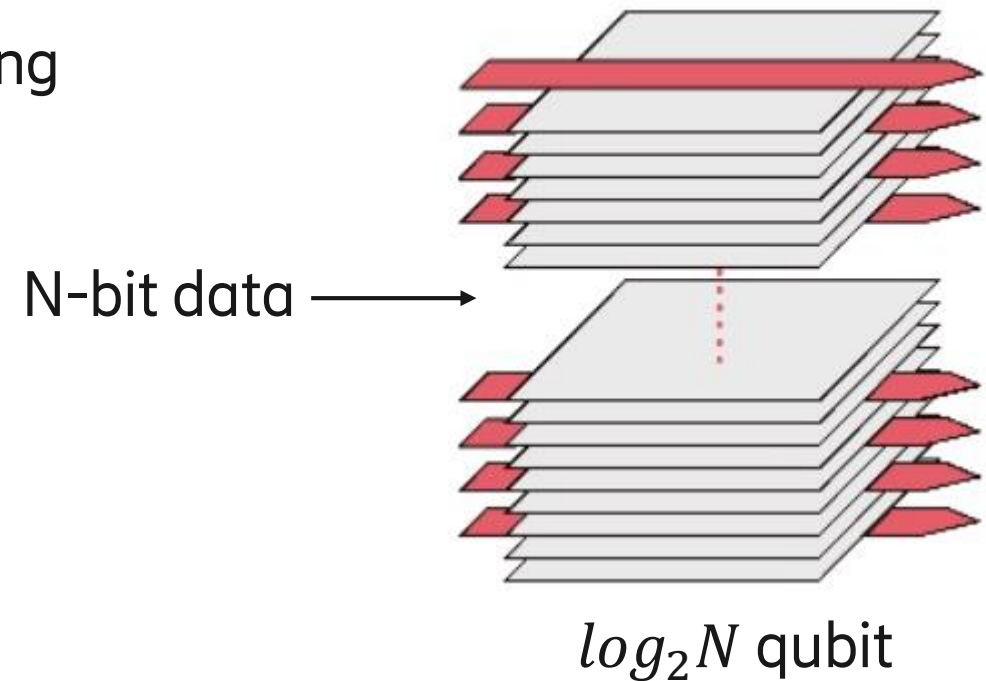
$$\begin{array}{l} 1529 \div 3 = 509 \dots\dots 2 \\ 1529 \div 5 = 305 \dots\dots 4 \\ 1529 \div 7 = 218 \dots\dots 3 \\ 1529 \div 11 = 139 \end{array} \left. \vphantom{\begin{array}{l} 1529 \div 3 = 509 \dots\dots 2 \\ 1529 \div 5 = 305 \dots\dots 4 \\ 1529 \div 7 = 218 \dots\dots 3 \\ 1529 \div 11 = 139 \end{array}} \right\} \text{Shor's Algorithm}$$

300-bit large integer factorization  $\begin{cases} \rightarrow 150,000 \text{ years} \\ \rightarrow 1 \text{ second} \end{cases}$

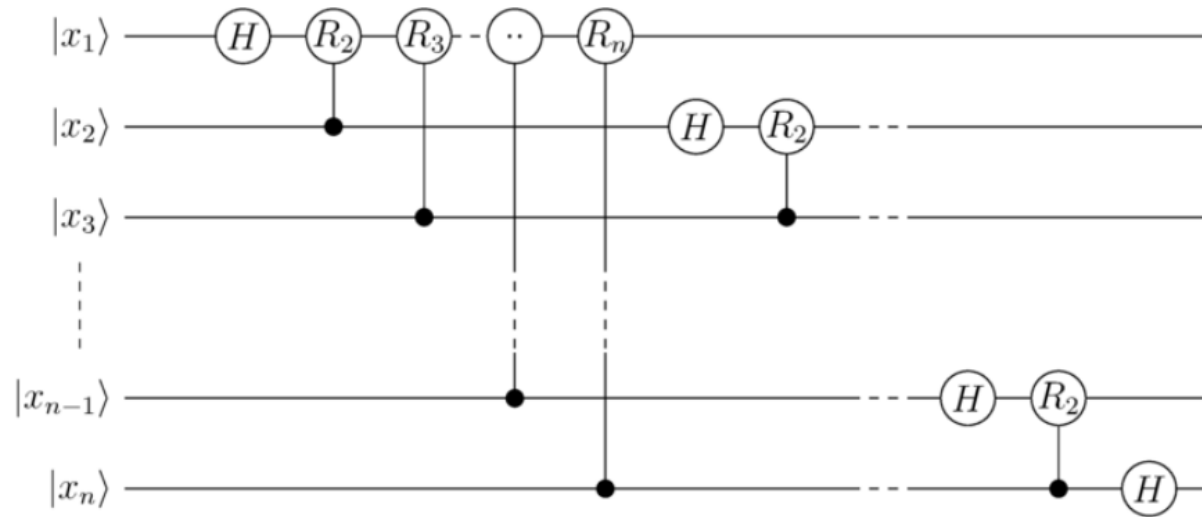
# Possibilities of Quantum Computing

Parallel computing → Large compute power

- Bit coins
- Database search: Grover's Algorithm
- Quantum computing + Machine learning
- Quantum Fourier transform



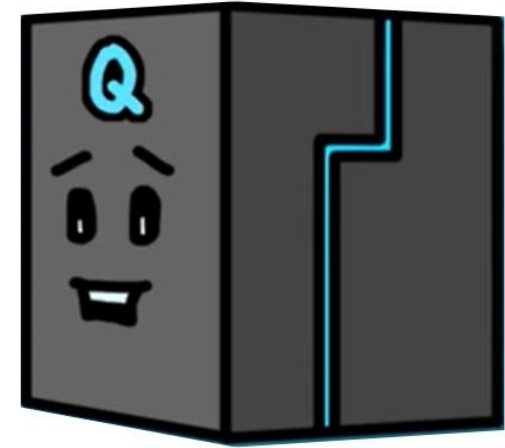
# Limitation of Quantum Computing



100 qubits

logical qubit (theoretical ideal)

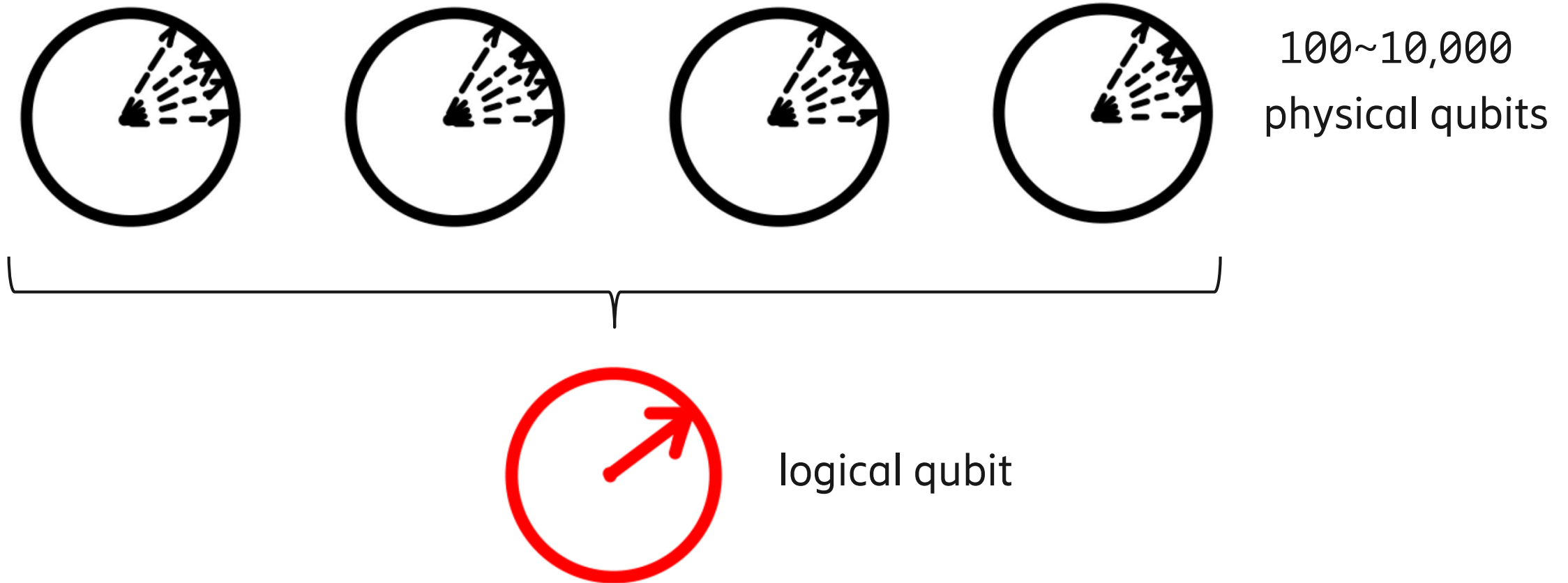
$\neq$



100 qubits

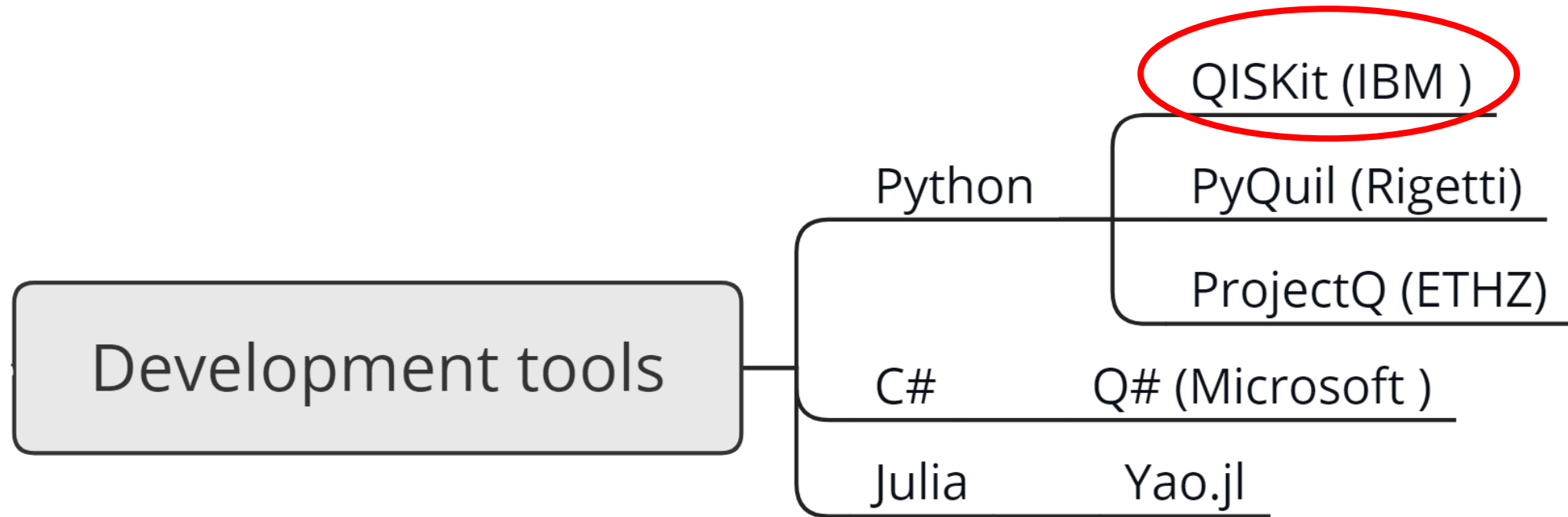
physical qubit (with noise)

# Limitation of Quantum Computing



Quantum Error Correction

# The Realization of Quantum Algorithms

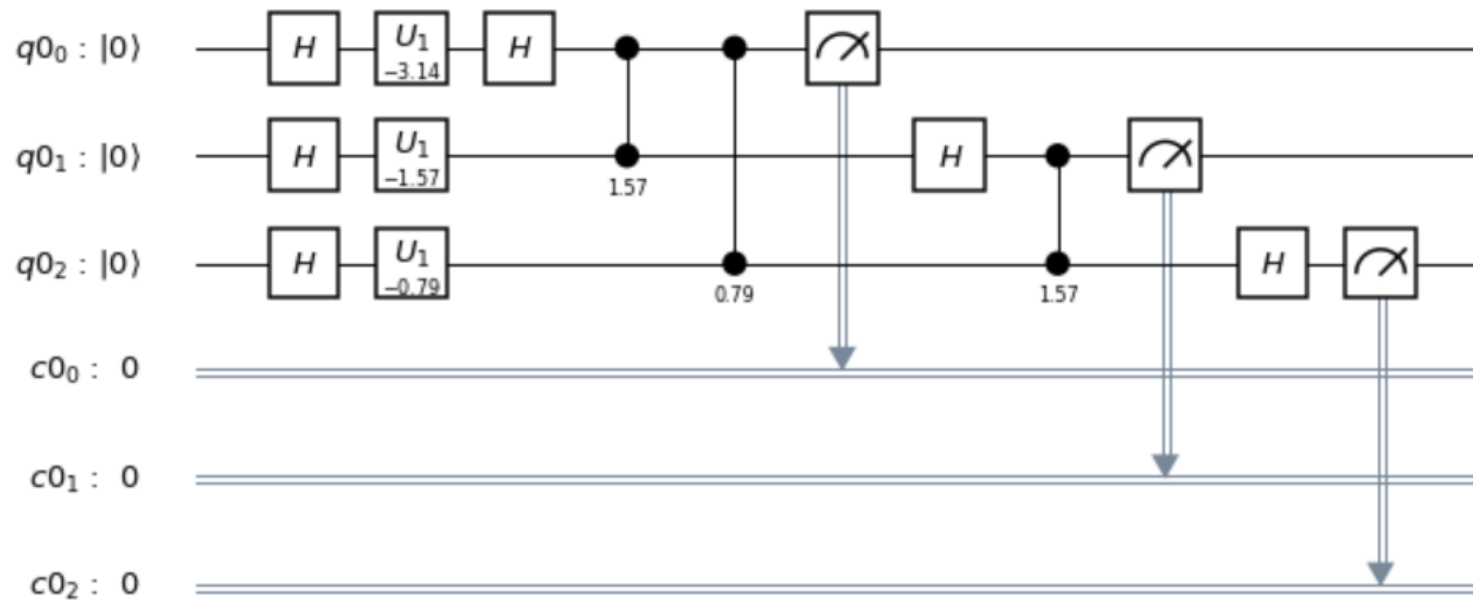




# The Realization of Quantum Algorithms

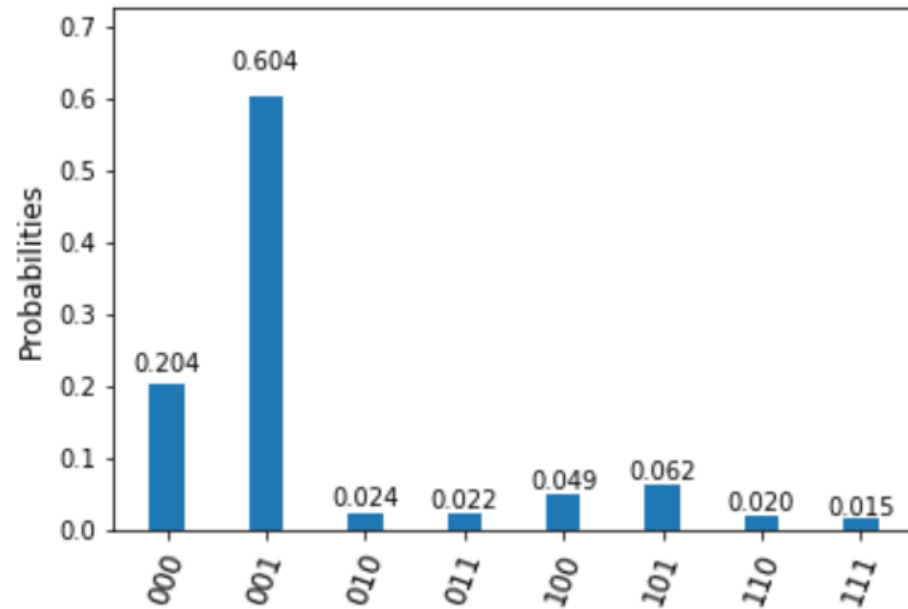
```
In [6]: # Visualizing quantum circuit
from qiskit.tools.visualization import circuit_drawer
circuit_drawer(qft_n)
```

WARNING: Unable to compile latex. Is `pdflatex` installed? Skipping latex circuit drawing...



# The Realization of Quantum Algorithms

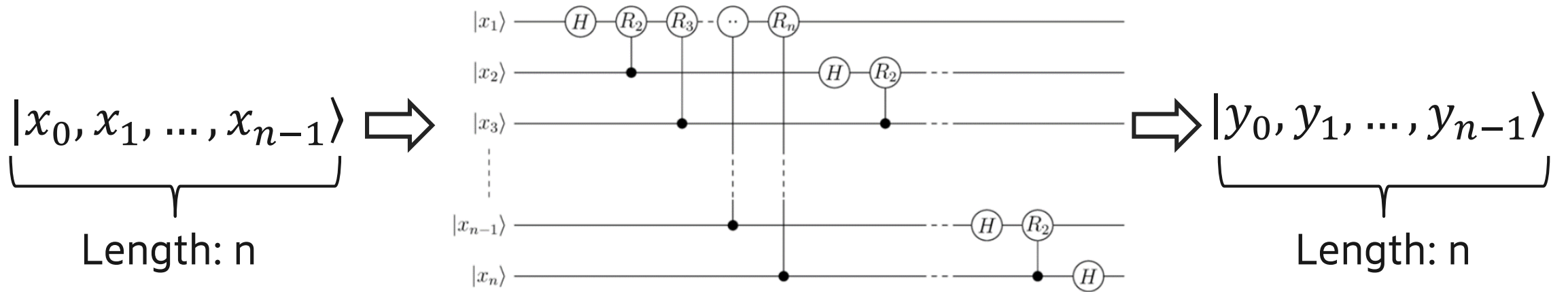
```
In [8]: results = job_exp.result()  
plot_histogram(results.get_counts())
```



Matplotlib

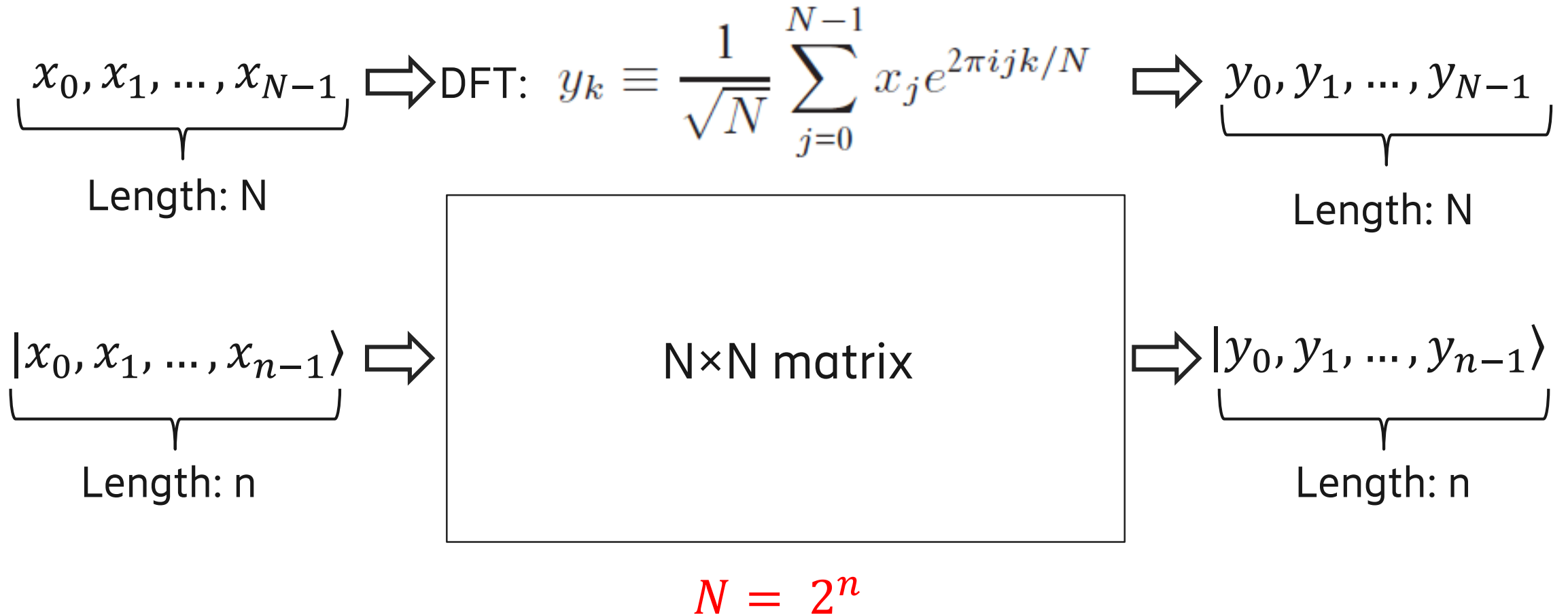
# The Realization of Quantum Fourier Transform

$$\underbrace{x_0, x_1, \dots, x_{N-1}}_{\text{Length: } N} \Rightarrow \text{DFT: } y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j k / N} \Rightarrow \underbrace{y_0, y_1, \dots, y_{N-1}}_{\text{Length: } N}$$



$$N = 2^n$$

# The Realization of Quantum Fourier Transform



# The Realization of Quantum Fourier Transform

