

QUANTUM COMPUTING

Ou au moins, ce que j'en ai compris...

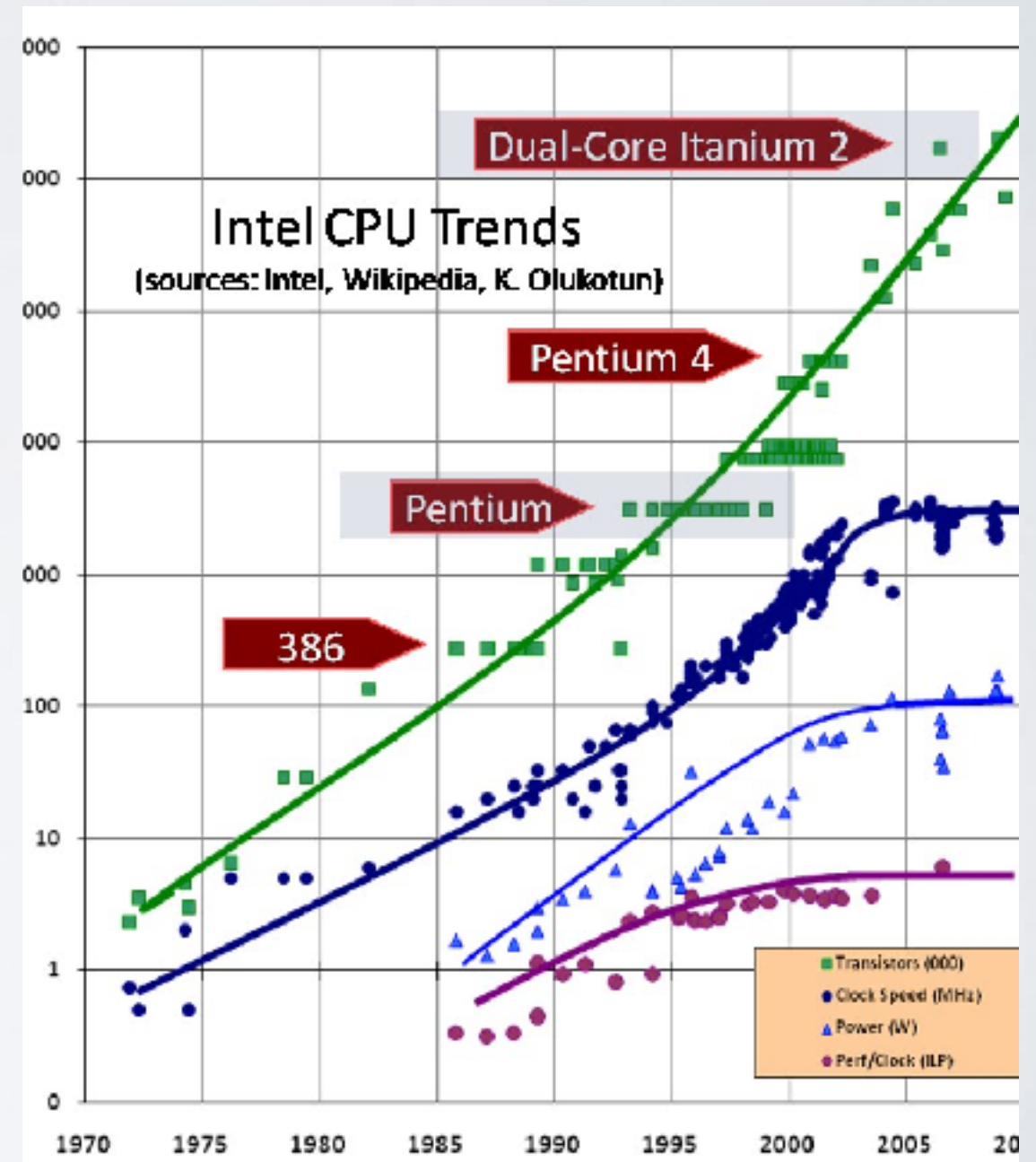
Jean-Philippe.Farrugia@univ-lyon1.fr



DISCLAIMER !

POURQUOI ?

- La loi de Moore atteindra bientôt une limite physique :
- Finesse de gravure du silicium.
- Changer de paradigme ? De technologie ?

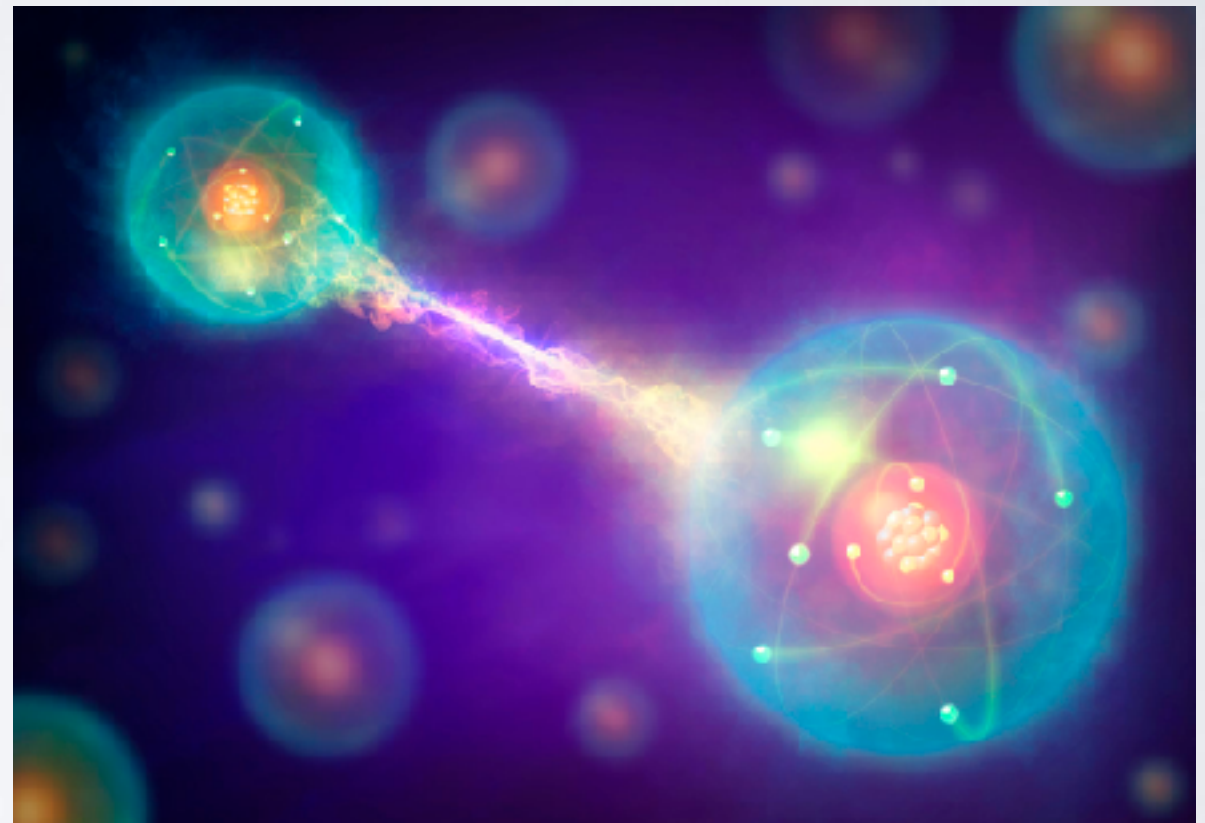


POURQUOI ?

- Tout le monde s'y met :
 - Google.
 - IBM.
 - Microsoft.
 - Échéances proches !
 - *The next big thing ?*

COMMENT ?

- Exploiter les caractéristiques quantiques des particules.
- Un nouveau type de parallélisme.
- Objectif : la suprématie quantique.



COMMENT ?

COMMENT ?



COMMENT ?



PLAN

- Quelques concepts de physique quantique.
- Fondements mathématiques.
- Les algorithmes classiques.
- Outils matériels et logiciels
- Perspectives

PLAN

- Quelques concepts de physique quantique.
- Fondements mathématiques.
- Les algorithmes classiques.
- Les principaux acteurs industriels.
- Perspectives

PHYSIQUE QUANTIQUE

- Objectif : description d'un micro-état.
- 3 concepts clés :
 - Dualité onde-corpuscule.
 - Superposition d'états.
 - Intrication.

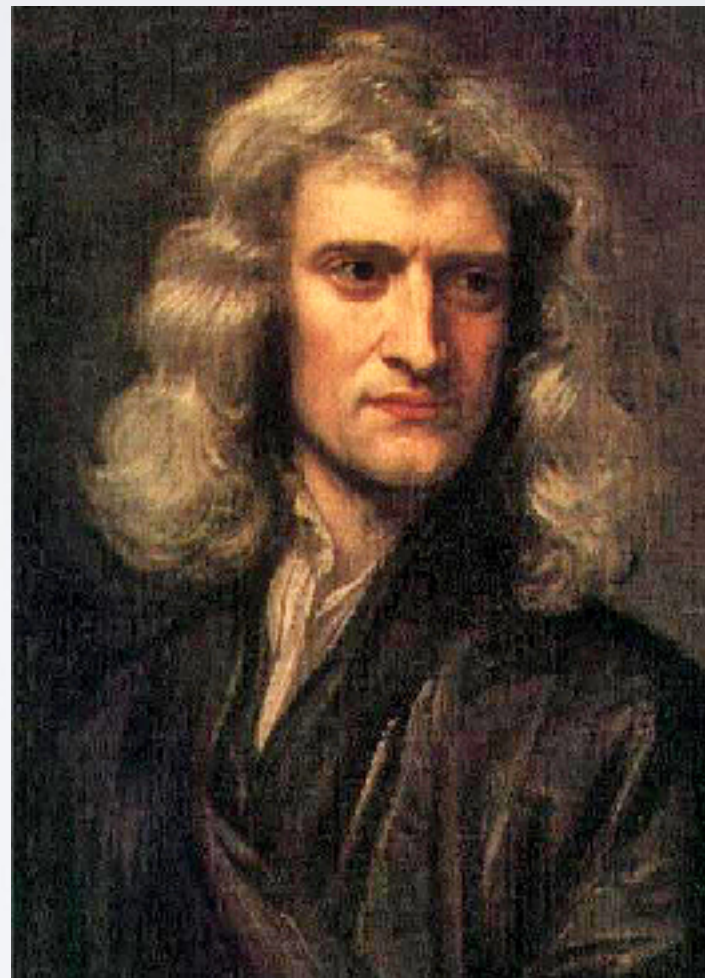
ORIGINE

- La nature de la lumière :
 - Corpuscule ?
 - Onde ?

Source : Wikipedia

ORIGINE

- La nature de la lumière :
- Corpuscule ?
- Onde ?

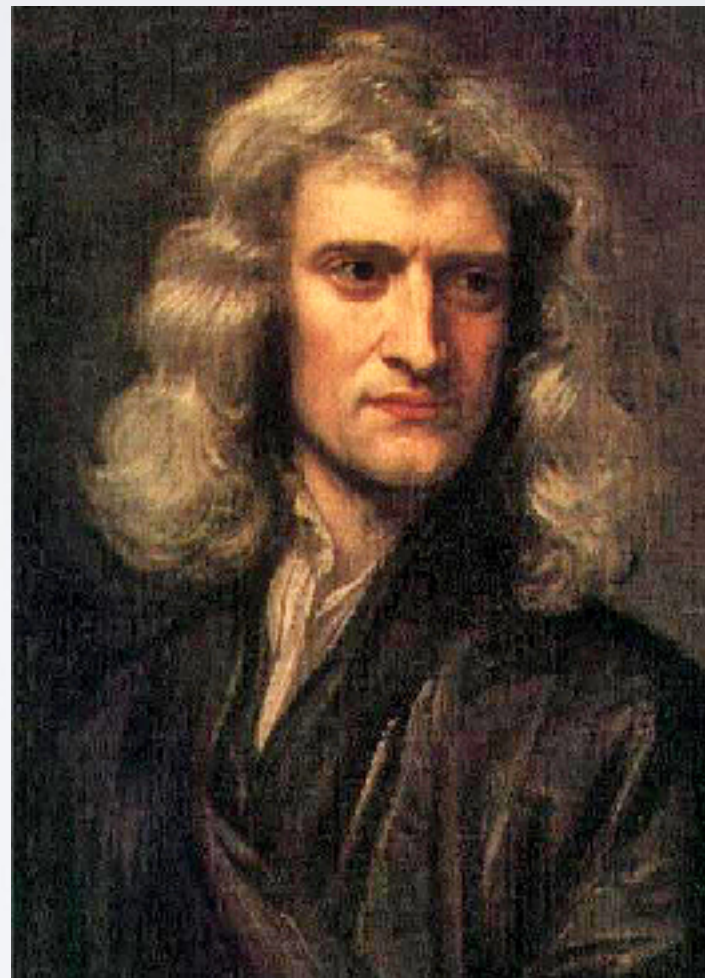


Isaac Newton

Source : Wikipedia

ORIGINE

- La nature de la lumière :
 - Corpuscule ?
 - Onde ?



Isaac Newton



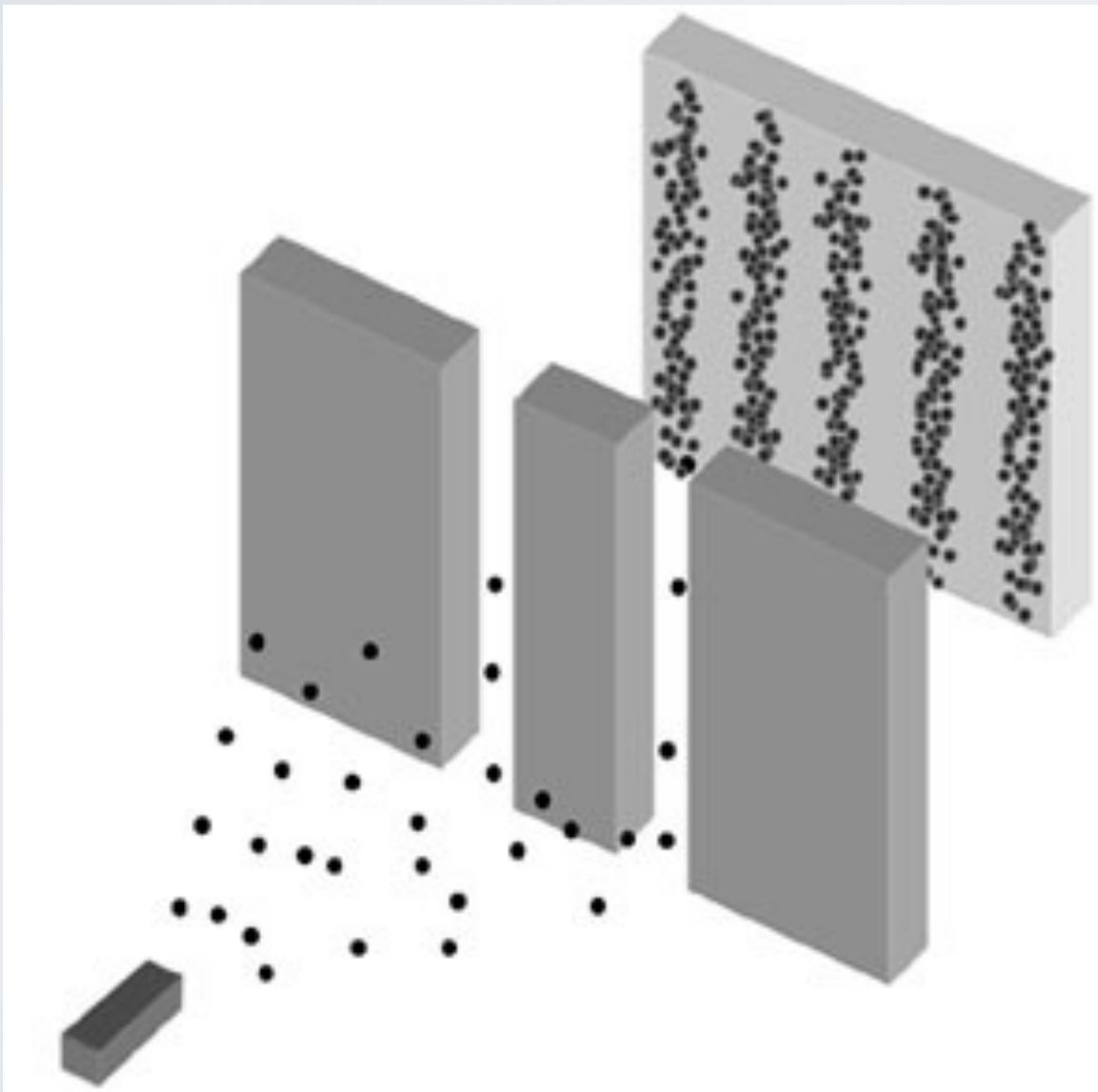
Christian Huygens

Source : Wikipedia

ONDE OU CORPUSCULE ?

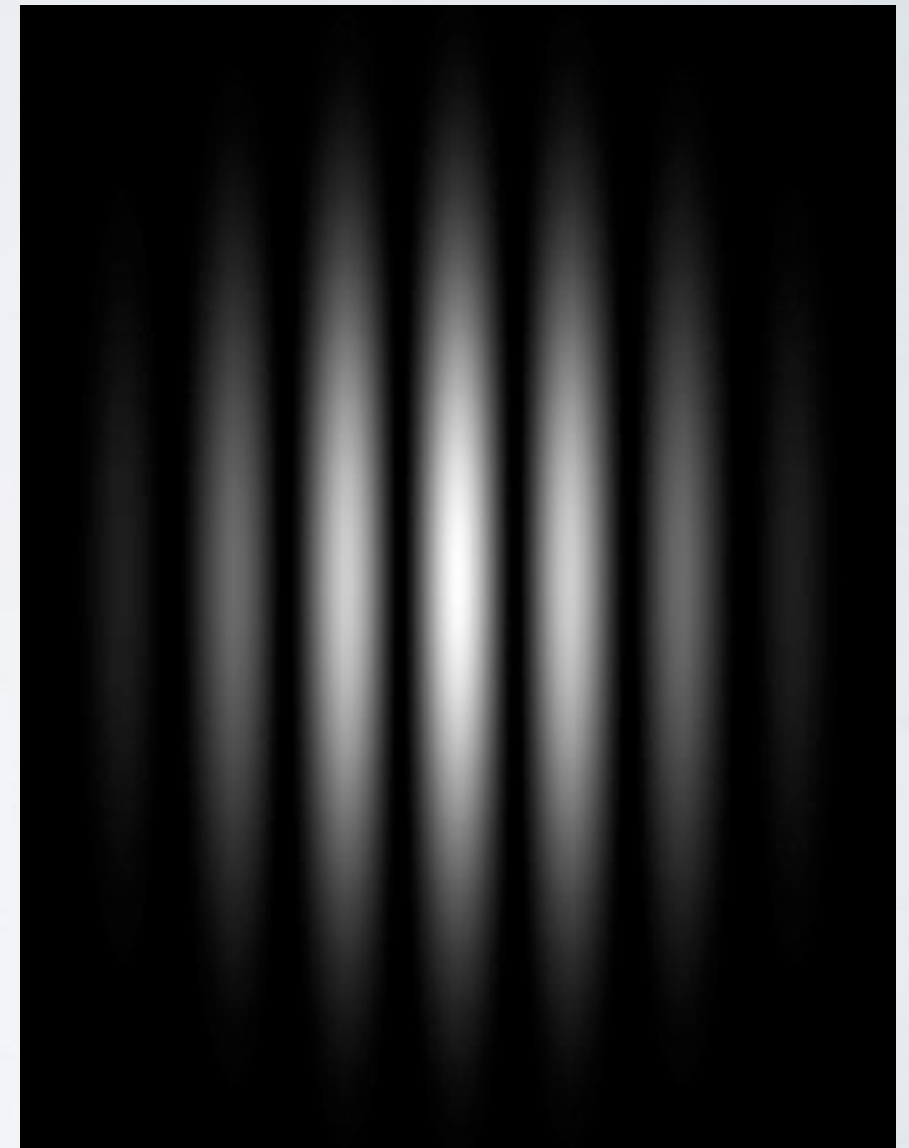
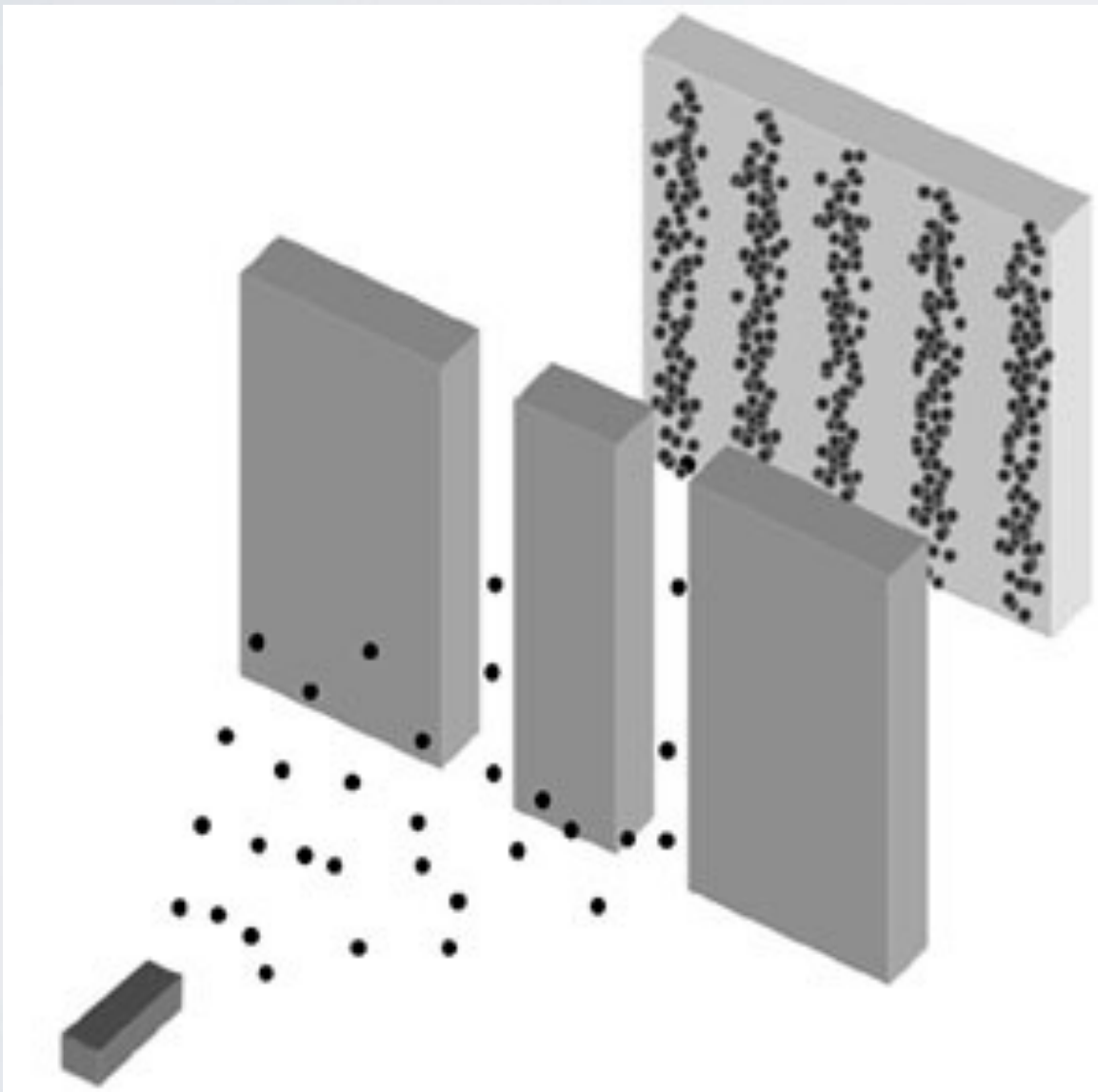
Source : Wikipedia

ONDE OU CORPUSCULE ?



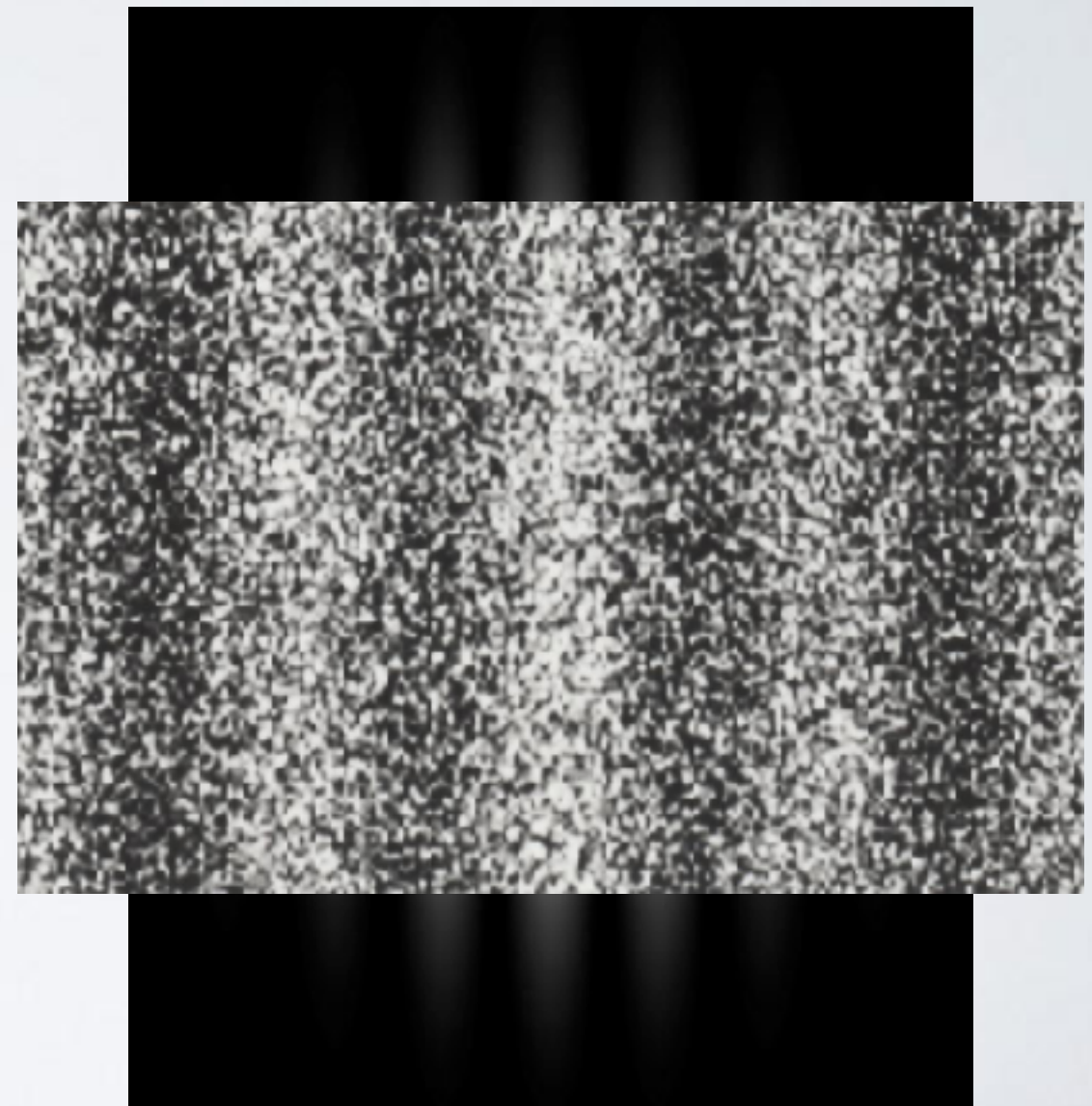
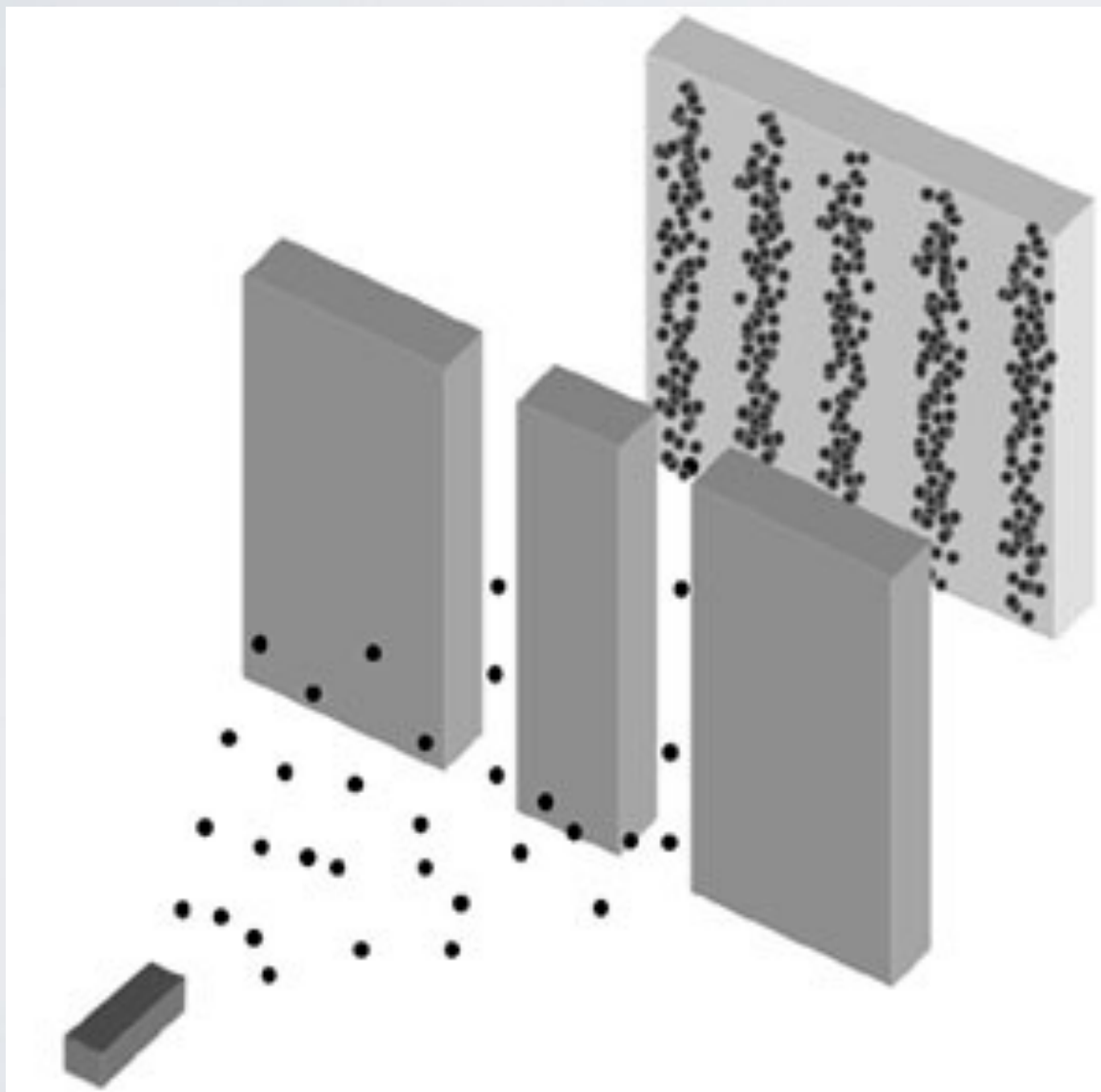
Source : Wikipedia

ONDE OU CORPUSCULE ?



Source : Wikipedia

ONDE OU CORPUSCULE ?



Source : Wikipedia

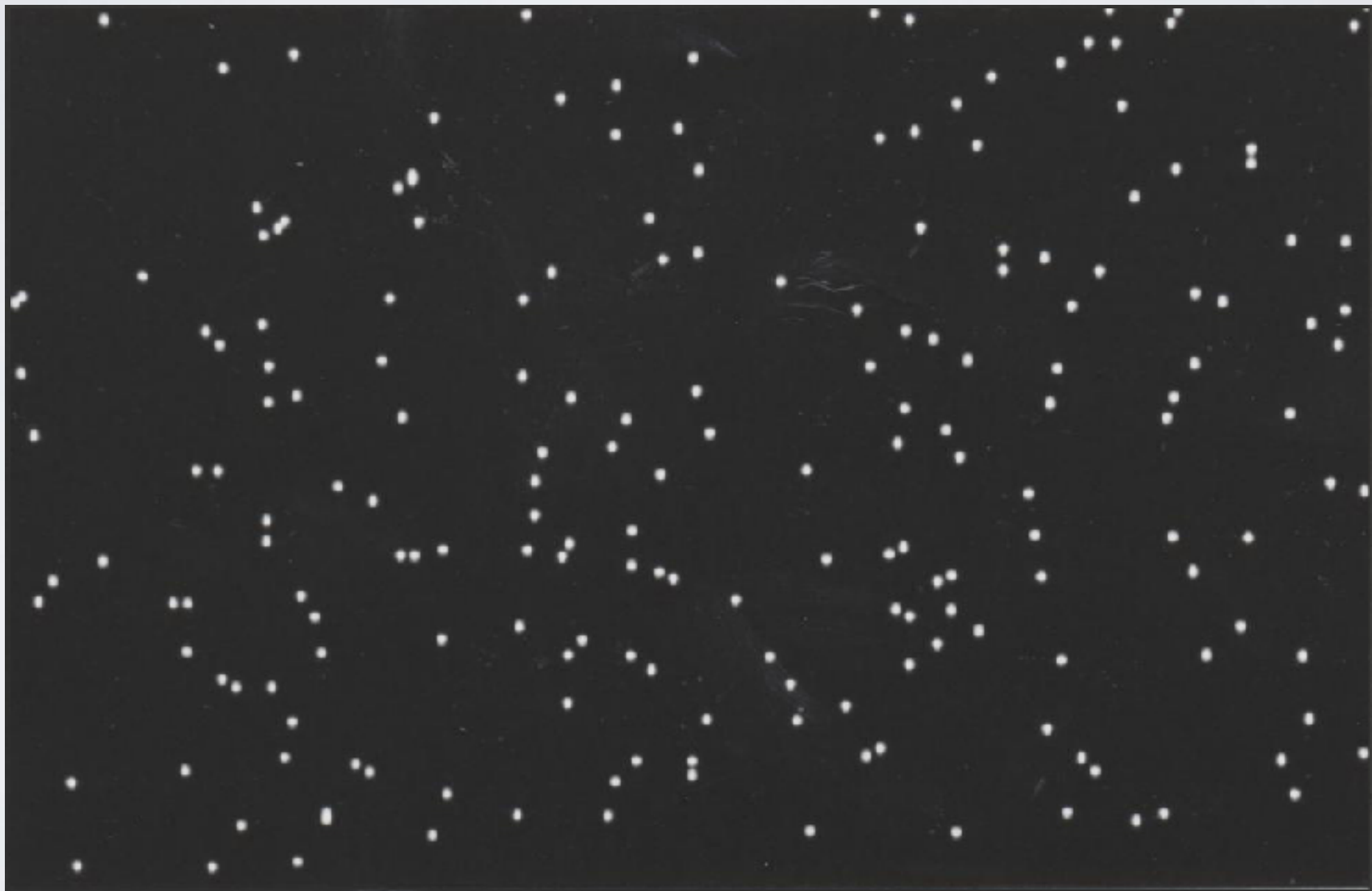
ONDE OU CORPUSCULE ?

ONDE OU CORPUSCULE ?



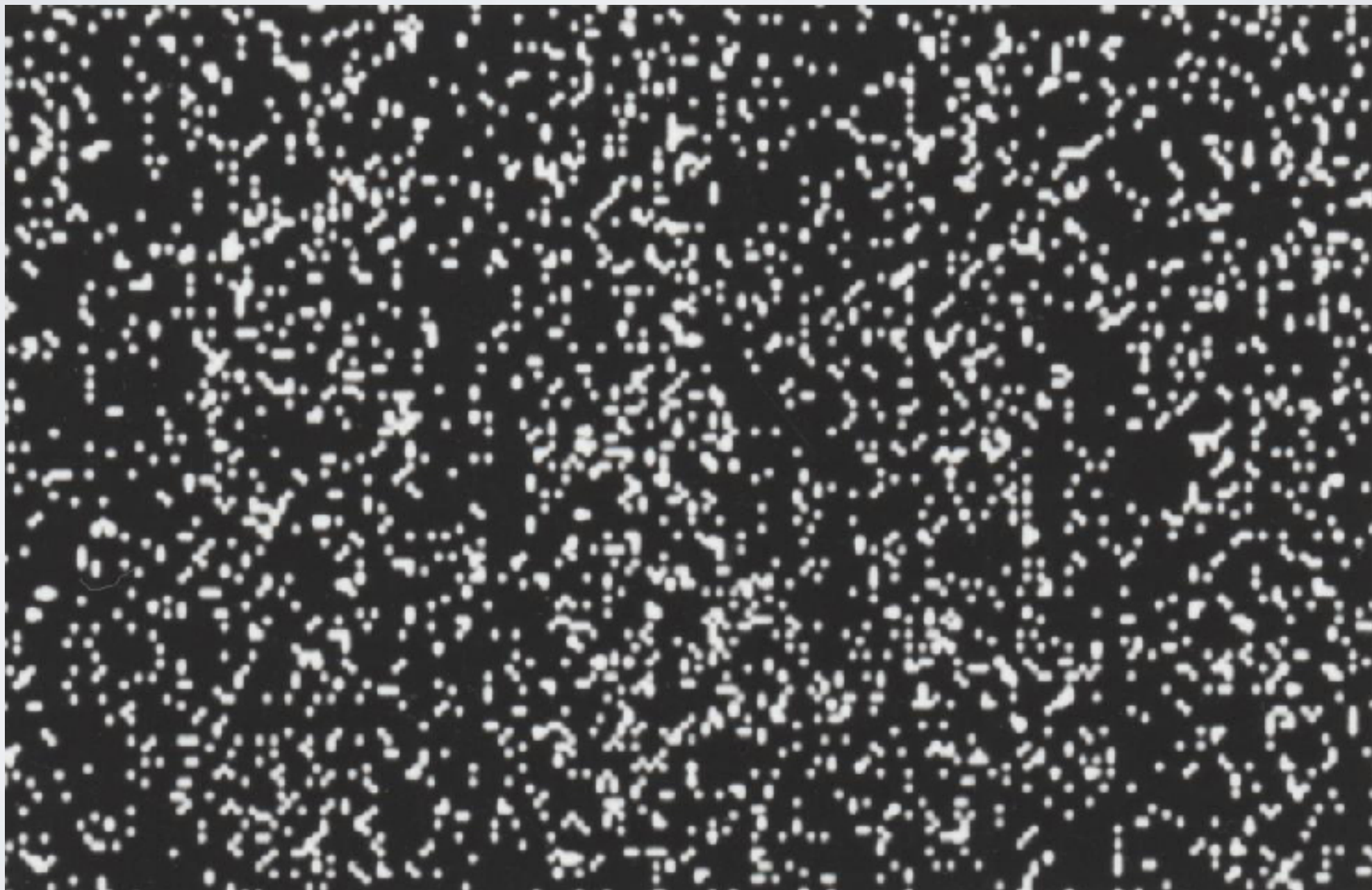
Source : Wikipedia

ONDE OU CORPUSCULE ?



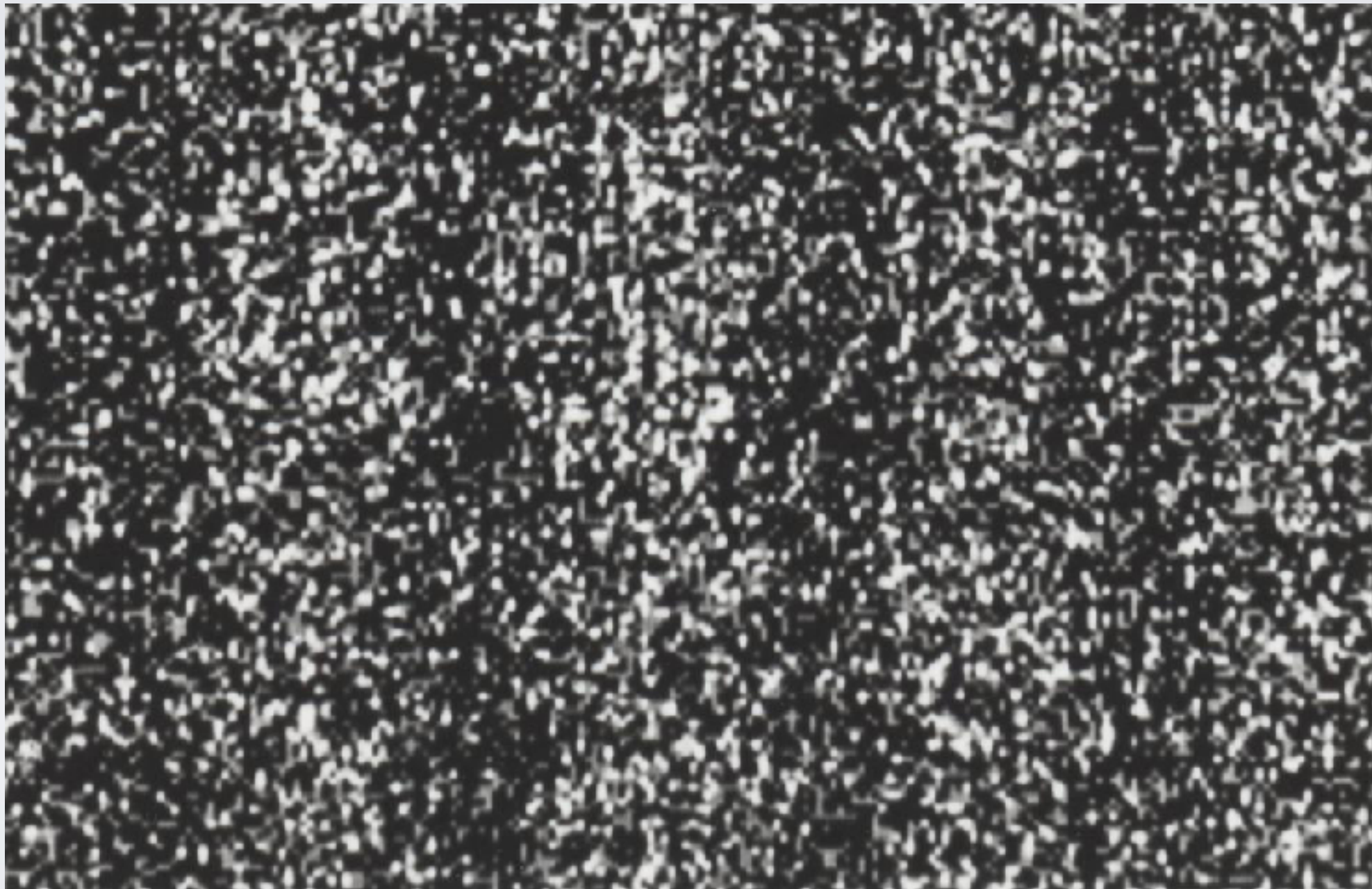
Source : Wikipedia

ONDE OU CORPUSCULE ?



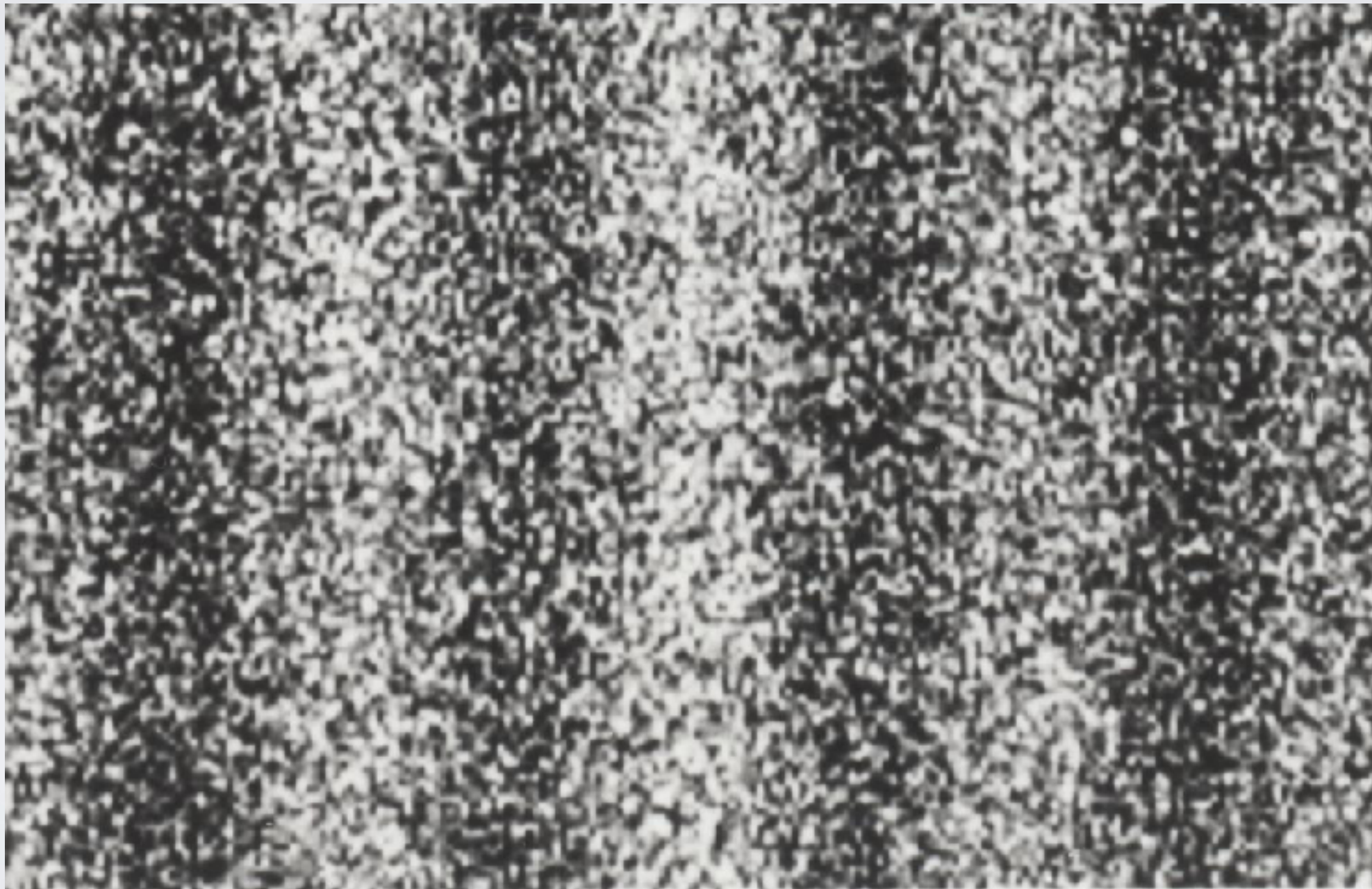
Source : Wikipedia

ONDE OU CORPUSCULE ?



Source : Wikipedia

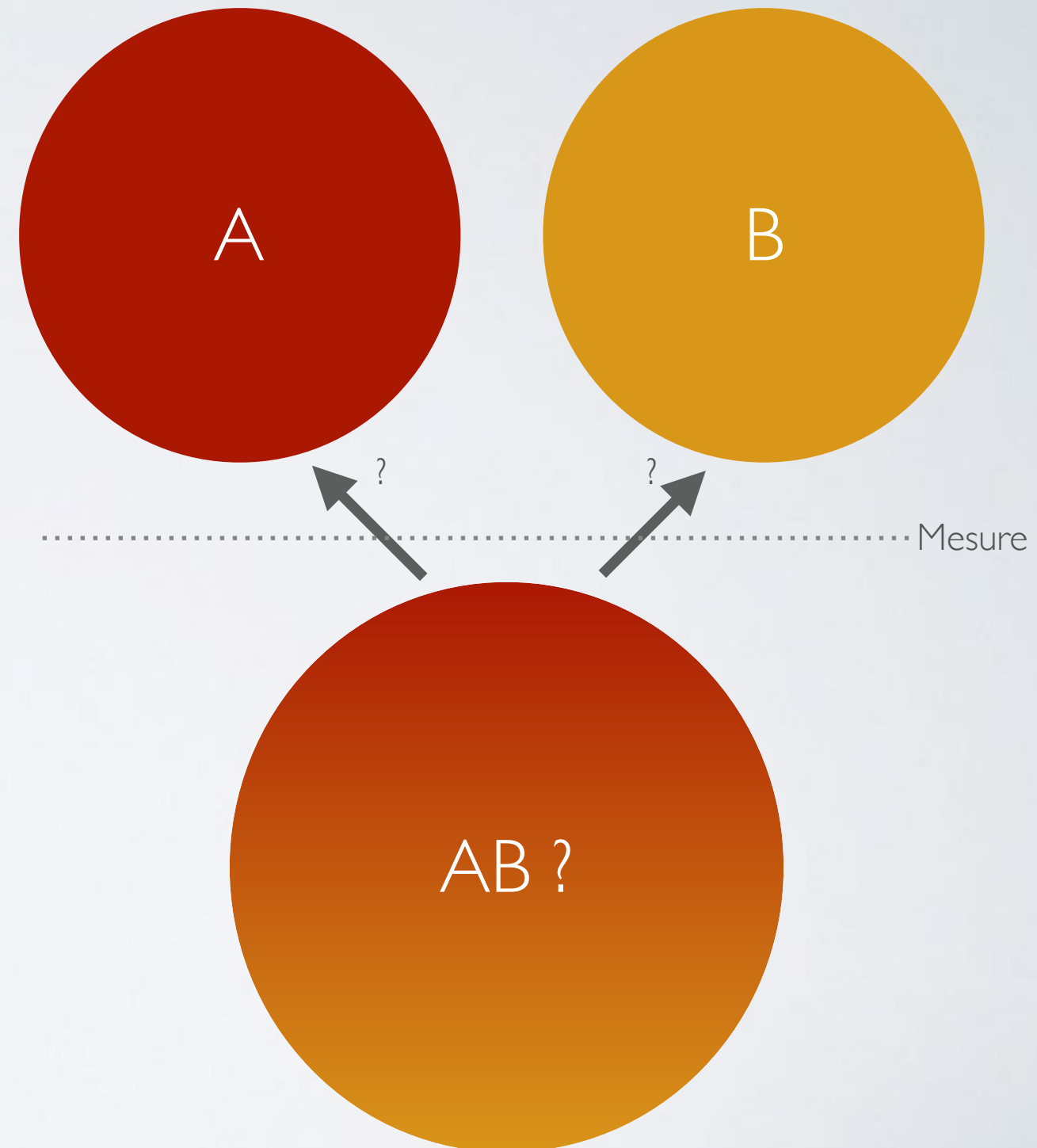
ONDE OU CORPUSCULE ?



Source : Wikipedia

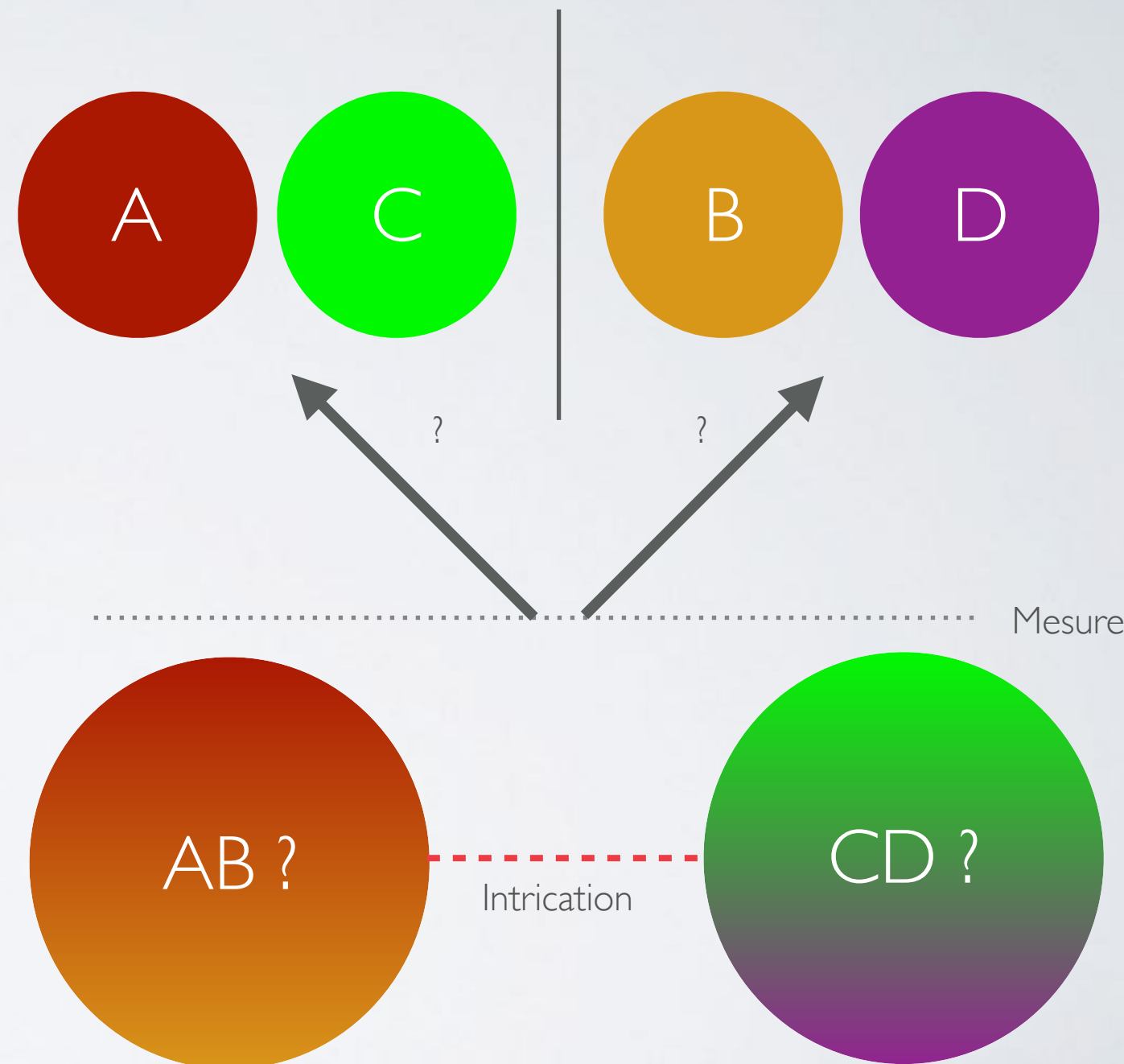
SUPERPOSITION D'ÉTATS

- Un système quantique peut être dans plusieurs états « en même temps » tant qu'on ne « mesure pas ».
- Mesure = dégénérescence aléatoire dans un état.
- Suit la PDF définie par une *fonction d'onde*.



INTRICATION

- Etat corrélé d'un système multiple :
- L'état de l'un dépend de l'autre, et réciproquement.



VERS L'INFORMATIQUE QUANTIQUE



Source : Wikipedia

VERS L'INFORMATIQUE QUANTIQUE

- 1982 : idée de R. Feynman :



Source : Wikipedia

VERS L'INFORMATIQUE QUANTIQUE

- 1982 : idée de R. Feynman :
- Les systèmes quantiques sont complexes à simuler.



Source : Wikipedia

VERS L'INFORMATIQUE QUANTIQUE

- 1982 : idée de R. Feynman :
- Les systèmes quantiques sont complexes à simuler.
- Peut-on les utiliser pour faire des calculs complexes ?



Source : Wikipedia

VERS L'INFORMATIQUE QUANTIQUE



Source : Ted Talks

VERS L'INFORMATIQUE QUANTIQUE

- 1985 : formalisation de D.
Deutsch :



Source : Ted Talks

VERS L'INFORMATIQUE QUANTIQUE

- 1985 : formalisation de D. Deutsch :
- Concevoir un *device* capable de simuler n'importe-quel système physique ?



Source : Ted Talks

VERS L'INFORMATIQUE QUANTIQUE

- 1985 : formalisation de D. Deutsch :
- Concevoir un *device* capable de simuler n'importe-quel système physique ?
- $\Rightarrow$ Un équivalent quantique de la machine de Turing.



Source : Ted Talks

VERS L'INFORMATIQUE QUANTIQUE

- 1985 : formalisation de D. Deutsch :
- Concevoir un *device* capable de simuler n'importe-quel système physique ?
 - $\Rightarrow$ Un équivalent quantique de la machine de Turing.
- Fondement théorique des machines quantiques actuelles.



Source : Ted Talks

PLAN

- Quelques concepts de physique quantique.
- Fondements mathématiques
- Les algorithmes classiques.
- Les principaux acteurs industriels.
- Perspectives

FONDEMENTS

FONDEMENTS

- Etat d'un système quantique décrit par une fonction d'onde complexe $\psi(r, t)$

FONDEMENTS

- Etat d'un système quantique décrit par une fonction d'onde complexe $\psi(r, t)$
 - Satisfait l'équation de Schrödinger.

FONDEMENTS

- Etat d'un système quantique décrit par une fonction d'onde complexe $\psi(r, t)$
 - Satisfait l'équation de Schrödinger.
 - Probabilité infinitésimale de réalisation de r : $|\psi(r, t)|^2 dr$

FONDEMENTS

- Etat d'un système quantique décrit par une fonction d'onde complexe $\psi(r, t)$
 - Satisfait l'équation de Schrödinger.
 - Probabilité infinitésimale de réalisation de r : $|\psi(r, t)|^2 dr$
 - De carré sommable : $\int |\psi(r, t)|^2 dr = 1$

FONDEMENTS

- Etat d'un système quantique décrit par une fonction d'onde complexe $\psi(r, t)$
 - Satisfait l'équation de Schrödinger.
 - Probabilité infinitésimale de réalisation de r : $|\psi(r, t)|^2 dr$
 - De carré sommable : $\int |\psi(r, t)|^2 dr = 1$
 - Sous-espace de L^2 .

FONDEMENTS

- Etat d'un système quantique décrit par une fonction d'onde complexe $\psi(r, t)$
 - Satisfait l'équation de Schrödinger.
 - Probabilité infinitésimale de réalisation de r : $|\psi(r, t)|^2 dr$
 - De carré sommable : $\int |\psi(r, t)|^2 dr = 1$
 - Sous-espace de L^2 .
- Produit scalaire sur cet espace : $(\phi, \psi) = \int \phi^*(r)\psi(r)dr$

FONDEMENTS

FONDEMENTS

- Base ortho-normée $U_i : \psi(r) = \sum_{i=0}^n C_i U_i(r)$

FONDEMENTS

- Base ortho-normée $U_i : \psi(r) = \sum_{i=0}^n C_i U_i(r)$
- Fonction d'onde $\Leftrightarrow$ vecteur «colonne » des C_i

FONDEMENTS

- Base ortho-normée $U_i : \psi(r) = \sum_{i=0}^n C_i U_i(r)$
 - Fonction d'onde $\Leftrightarrow$ vecteur «colonne » des C_i
 - Probabilité d'obtention de l'état $U_i : |C_i|^2$

FONDEMENTS

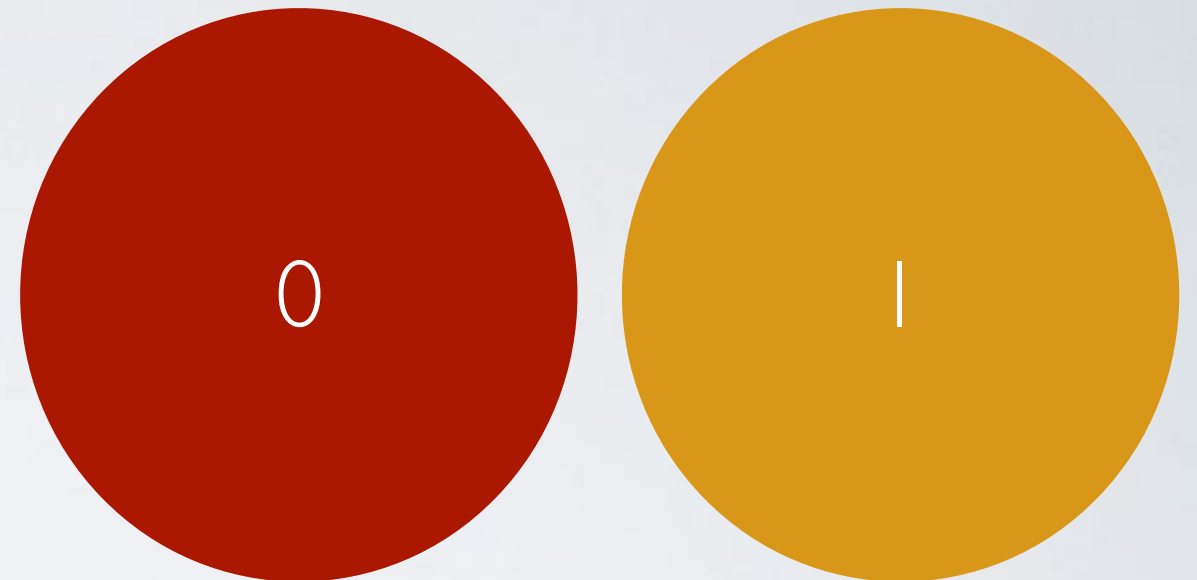
- Base ortho-normée $U_i : \psi(r) = \sum_{i=0}^n C_i U_i(r)$
 - Fonction d'onde $\Leftrightarrow$ vecteur «colonne » des C_i
 - Probabilité d'obtention de l'état $U_i : |C_i|^2$
- Des *opérateurs* unitaires (matrices unitaires) A .

FONDEMENTS

- Base ortho-normée $U_i : \psi(r) = \sum_{i=0}^n C_i U_i(r)$
 - Fonction d'onde $\Leftrightarrow$ vecteur «colonne » des C_i
 - Probabilité d'obtention de l'état $U_i : |C_i|^2$
- Des *opérateurs* unitaires (matrices unitaires) A .
- Des *fonctionnelles linéaires* (vecteurs « lignes »).

UN QBIT ?

- Equivalent quantique du bit.
- QBit : système quantique à deux niveaux.
- Deux états de base : 0 et 1.
- Pas nécessairement équiprobables !



Bit classique



QBit

QBIT - DIRAC

QBIT - DIRAC

- Un système à deux niveaux : $\psi(r) = C_0 U_0(r) + C_1 U_1(r)$

QBIT - DIRAC

- Un système à deux niveaux : $\psi(r) = C_0 U_0(r) + C_1 U_1(r)$
- Notation de Dirac

QBIT - DIRAC

- Un système à deux niveaux : $\psi(r) = C_0 U_0(r) + C_1 U_1(r)$
- Notation de Dirac
 - Bra : $|\psi\rangle = \text{Vecteur}$.

QBIT - DIRAC

- Un système à deux niveaux : $\psi(r) = C_0 U_0(r) + C_1 U_1(r)$
- Notation de Dirac
 - Bra : $|\psi\rangle = \text{Vecteur.}$
 - Ket : $\langle\phi| = \text{Fonctionnelle linéaire.}$

QBIT - DIRAC

- Un système à deux niveaux : $\psi(r) = C_0 U_0(r) + C_1 U_1(r)$
- Notation de Dirac
 - Bra : $|\psi\rangle = \text{Vecteur}$.
 - Ket : $\langle\phi| = \text{Fonctionnelle linéaire}$.
 - Produit scalaire : Bracket = $\langle\phi|\psi\rangle$

QBIT - DIRAC

- Un système à deux niveaux : $\psi(r) = C_0 U_0(r) + C_1 U_1(r)$
- Notation de Dirac
 - Bra : $|\psi\rangle = \text{Vecteur.}$
 - Ket : $\langle\phi| = \text{Fonctionnelle linéaire.}$
 - Produit scalaire : Bracket = $\langle\phi|\psi\rangle$
- Deux niveaux du Qbit : $|0\rangle$ et $|1\rangle$

QBIT - DIRAC

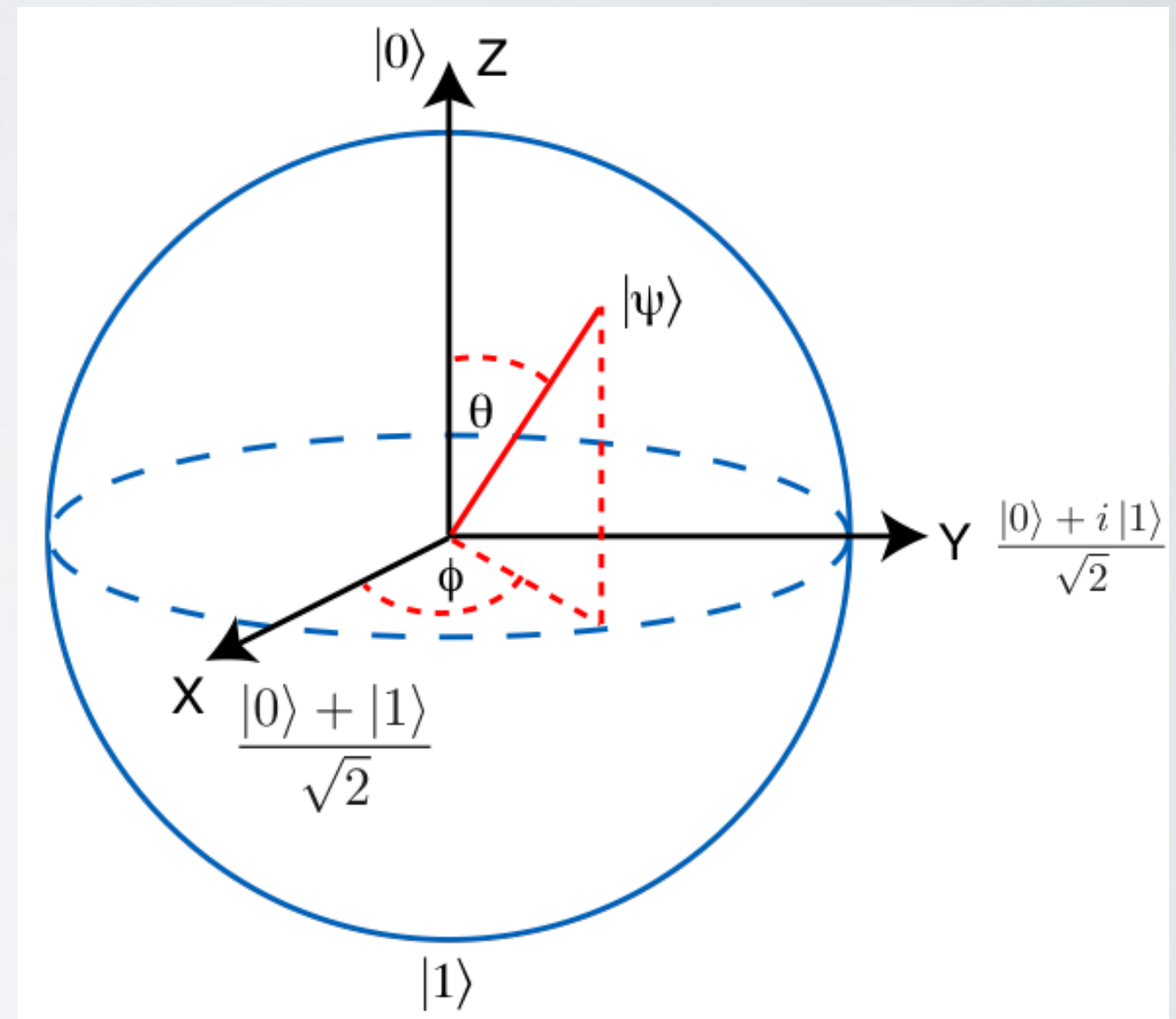
- Un système à deux niveaux : $\psi(r) = C_0 U_0(r) + C_1 U_1(r)$
- Notation de Dirac
 - Bra : $|\psi\rangle = \text{Vecteur}$.
 - Ket : $\langle\phi| = \text{Fonctionnelle linéaire}$.
 - Produit scalaire : Bracket = $\langle\phi|\psi\rangle$
- Deux niveaux du Qbit : $|0\rangle$ et $|1\rangle$
- Etat du QBit : combinaison linéaire de ces deux niveaux.

QBIT - DIRAC

- Un système à deux niveaux : $\psi(r) = C_0 U_0(r) + C_1 U_1(r)$
- Notation de Dirac
 - Bra : $|\psi\rangle = \text{Vecteur}$.
 - Ket : $\langle\phi| = \text{Fonctionnelle linéaire}$.
 - Produit scalaire : Bracket = $\langle\phi|\psi\rangle$
- Deux niveaux du Qbit : $|0\rangle$ et $|1\rangle$
- Etat du QBit : combinaison linéaire de ces deux niveaux.
 - $|\psi\rangle = C_0|0\rangle + C_1|1\rangle$

SPHÈRE DE BLOCH

- Représentation graphique de l'état d'un QBit.
- Tomographie complexe.



$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi} \sin(\theta/2)|1\rangle,$$

PORTES QUANTIQUES

- Opérateurs unitaires :

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- Matrice 2x2 unitaire A :

- $|\psi'\rangle = A|\psi\rangle$ avec $A^*A = I$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

- Opérateurs de Pauli X,Y,Z :

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- Rotation de π rad sur chaque axe.

- Opérateur Hadamard H:

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

- Provoquer une superposition d'état à partir d'un état stable.

PORTES QUANTIQUES

PORTES QUANTIQUES

- Pour visualiser :

PORTES QUANTIQUES

- Pour visualiser :
- $X(\alpha | 0 \rangle + \beta | 1 \rangle) = \beta | 0 \rangle + \alpha | 1 \rangle$

PORTES QUANTIQUES

- Pour visualiser :
- $X(\alpha |0\rangle + \beta |1\rangle) = \beta |0\rangle + \alpha |1\rangle$
- $Z(\alpha |0\rangle + \beta |1\rangle) = \alpha |0\rangle - \beta |1\rangle$

PORTES QUANTIQUES

- Pour visualiser :
- $X(\alpha | 0 \rangle + \beta | 1 \rangle) = \beta | 0 \rangle + \alpha | 1 \rangle$
- $Z(\alpha | 0 \rangle + \beta | 1 \rangle) = \alpha | 0 \rangle - \beta | 1 \rangle$
- $H(\alpha | 0 \rangle + \beta | 1 \rangle) = \frac{\alpha + \beta}{\sqrt{2}} | 0 \rangle + \frac{\alpha - \beta}{\sqrt{2}} | 1 \rangle$

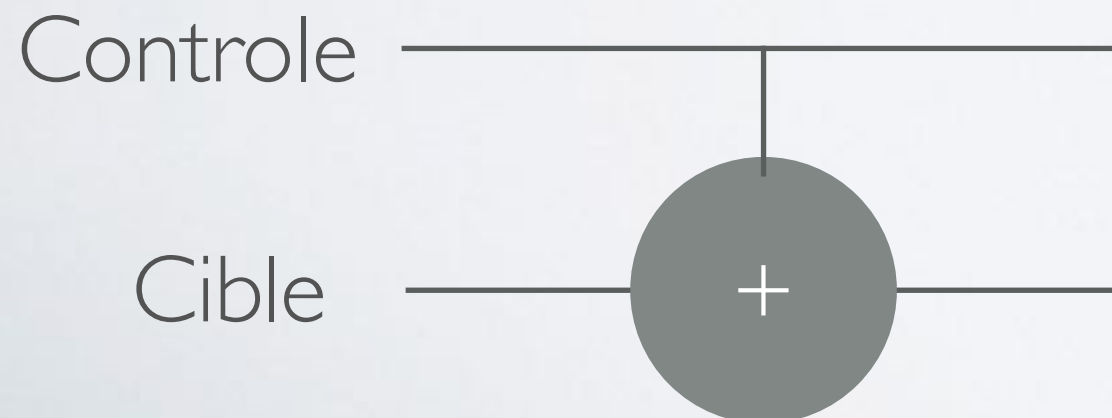
PORTES MULTIPLES

- Pour des systèmes quantique à QBits multiples.

Exemple : Base d'un système à 2 QBits

$$\{ |00\rangle, |01\rangle, |10\rangle, |11\rangle \}$$

- Porte Conditional Not (CNOT) :



$$U_{CN} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

PORTES MULTIPLES

PORTES MULTIPLES

- Pour visualiser : CNOT sur les vecteurs de la base.

PORTES MULTIPLES

- Pour visualiser : CNOT sur les vecteurs de la base.
- $U_{CN}(|00\rangle) = |00\rangle$

PORTES MULTIPLES

- Pour visualiser : CNOT sur les vecteurs de la base.
- $U_{CN}(|00\rangle) = |00\rangle$
- $U_{CN}(|01\rangle) = |01\rangle$

PORTES MULTIPLES

- Pour visualiser : CNOT sur les vecteurs de la base.
- $U_{CN}(|00\rangle) = |00\rangle$
- $U_{CN}(|01\rangle) = |01\rangle$
- $U_{CN}(|10\rangle) = |11\rangle$

PORTES MULTIPLES

- Pour visualiser : CNOT sur les vecteurs de la base.

- $U_{CN}(|00\rangle) = |00\rangle$

- $U_{CN}(|01\rangle) = |01\rangle$

- $U_{CN}(|10\rangle) = |11\rangle$

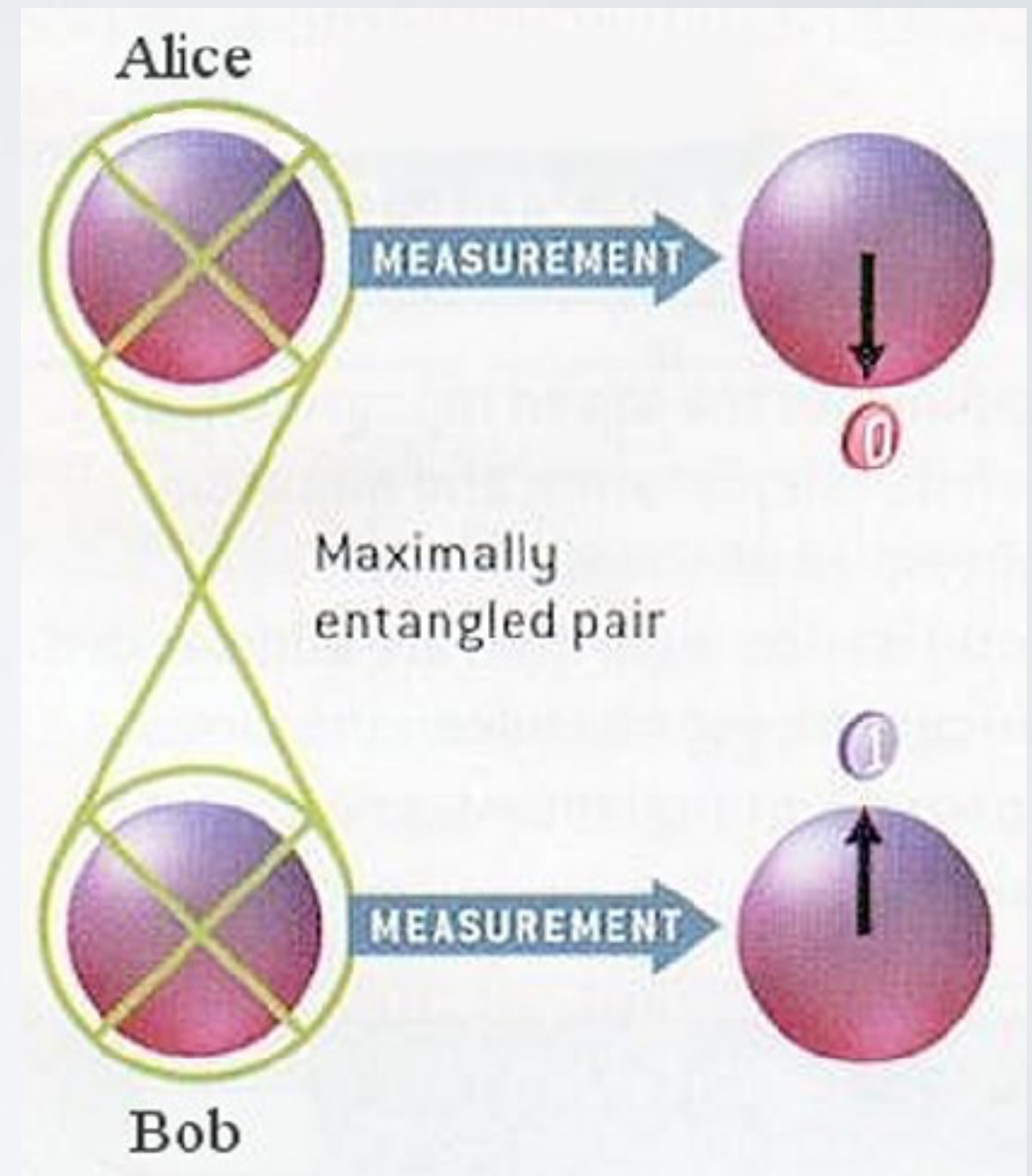
- $U_{CN}(|11\rangle) = |10\rangle$

INTRICATION

- Systeme à QBit multiple dans lequel chaque état ne peut être décrit comme une combinaison de QBits indépendants.

- $(|00\rangle + |01\rangle)/\sqrt{2}$

- $(|01\rangle + |10\rangle)/\sqrt{2}$

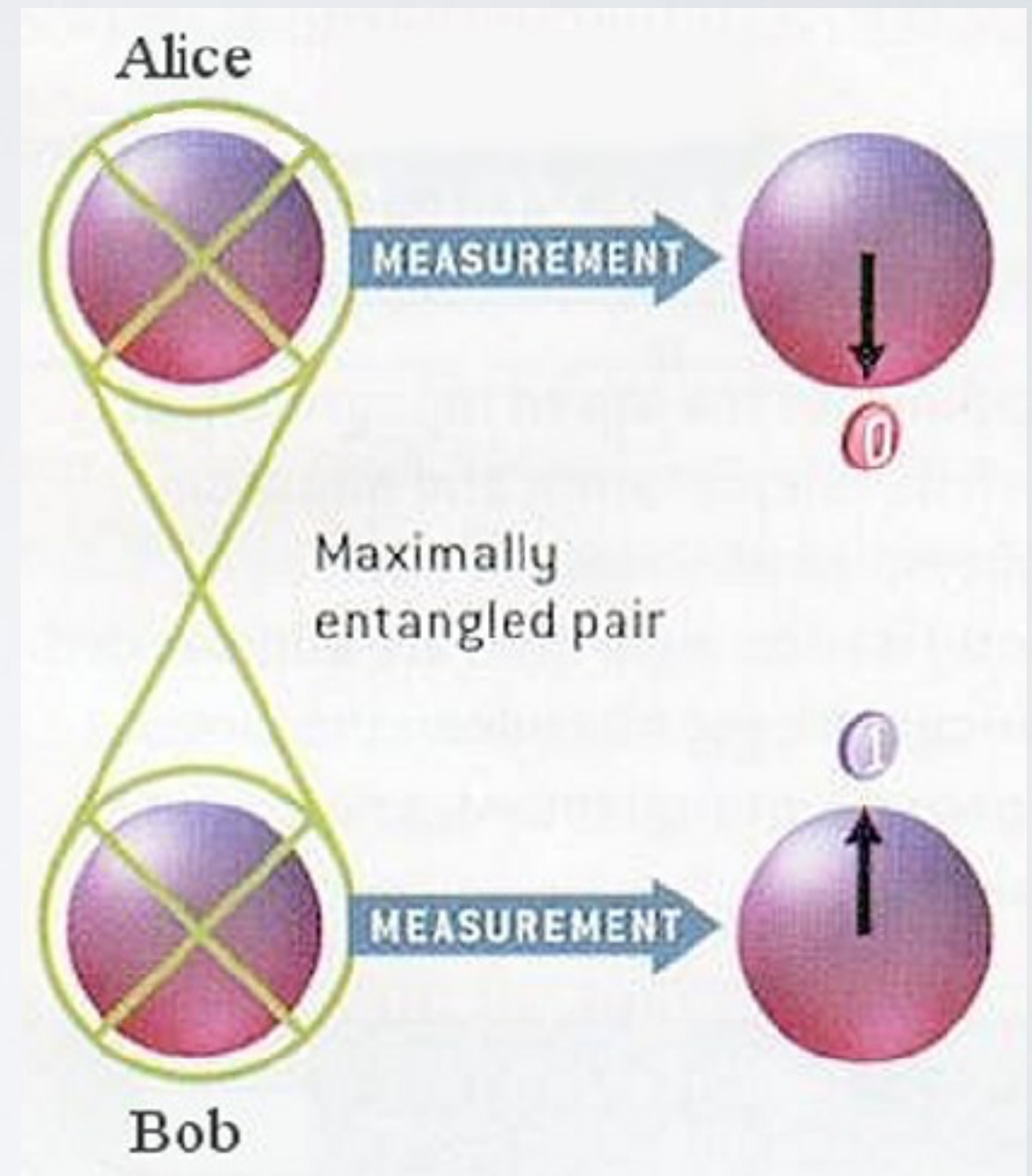


INTRICATION

- Systeme à QBit multiple dans lequel chaque état ne peut être décrit comme une combinaison de QBits indépendants.

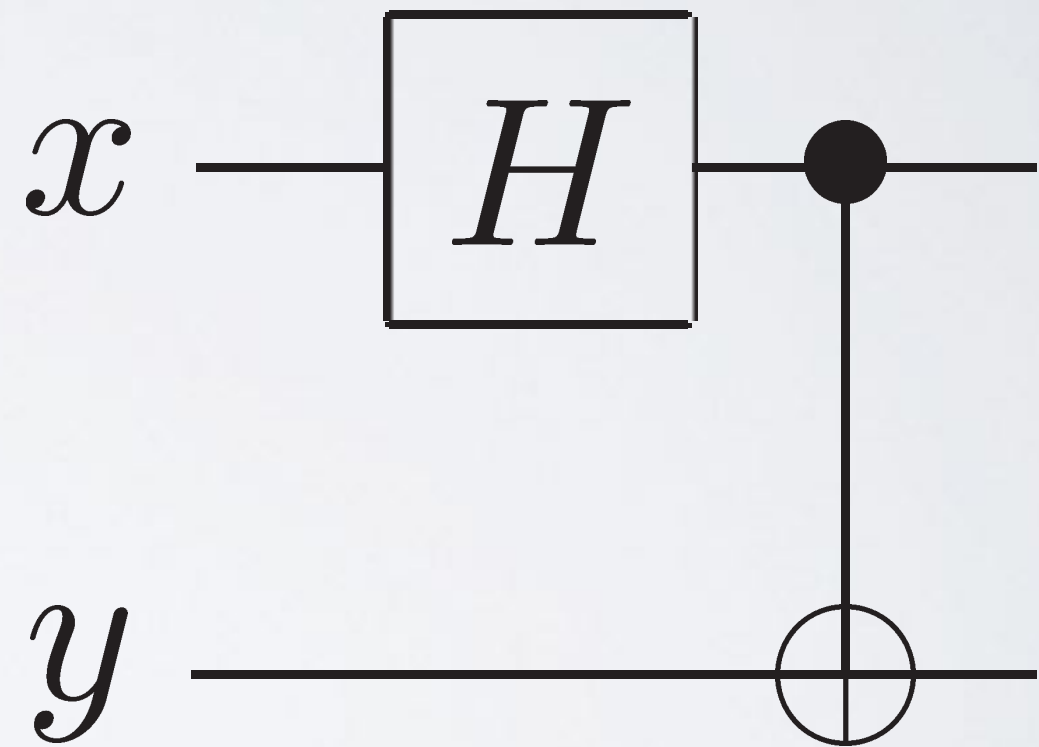
- ~~$(|00\rangle + |01\rangle)/\sqrt{2}$~~

- $(|01\rangle + |10\rangle)/\sqrt{2}$



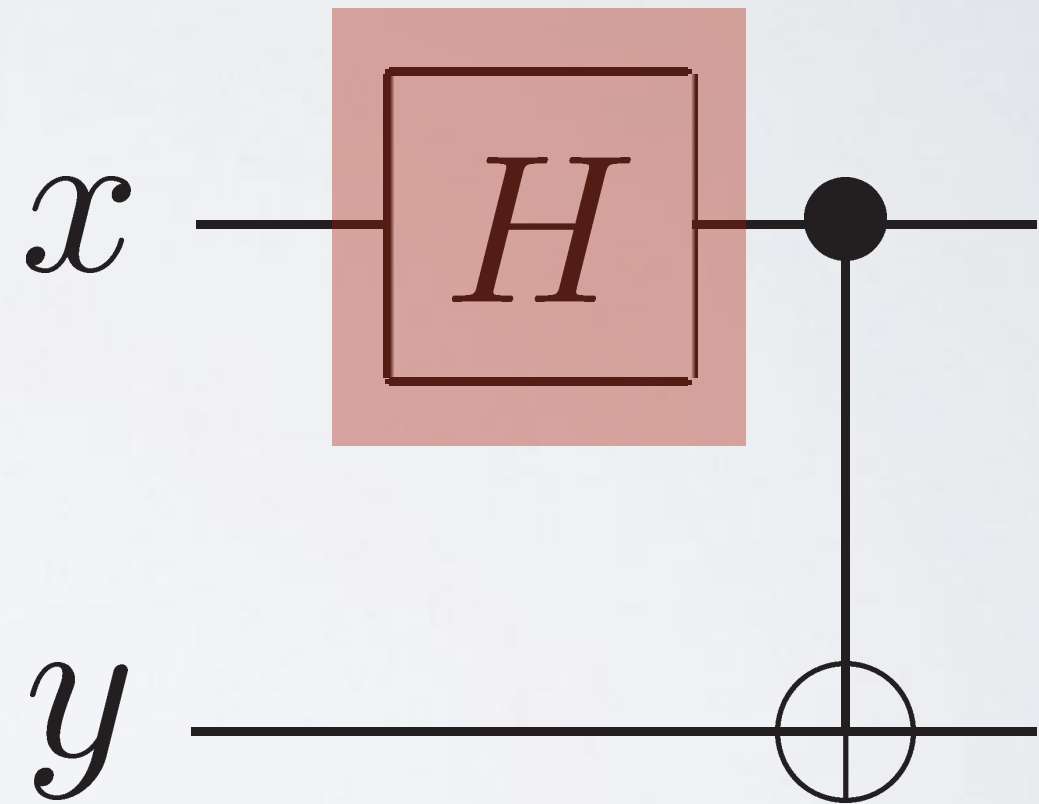
PROGRAMME QUANTIQUE

- Un enchainement de porte quantiques.
- Peut être représenté graphiquement.
 - Plus facile quand on a plusieurs QBits.
- Exemple : obtention d'un *Etat de Bell* :



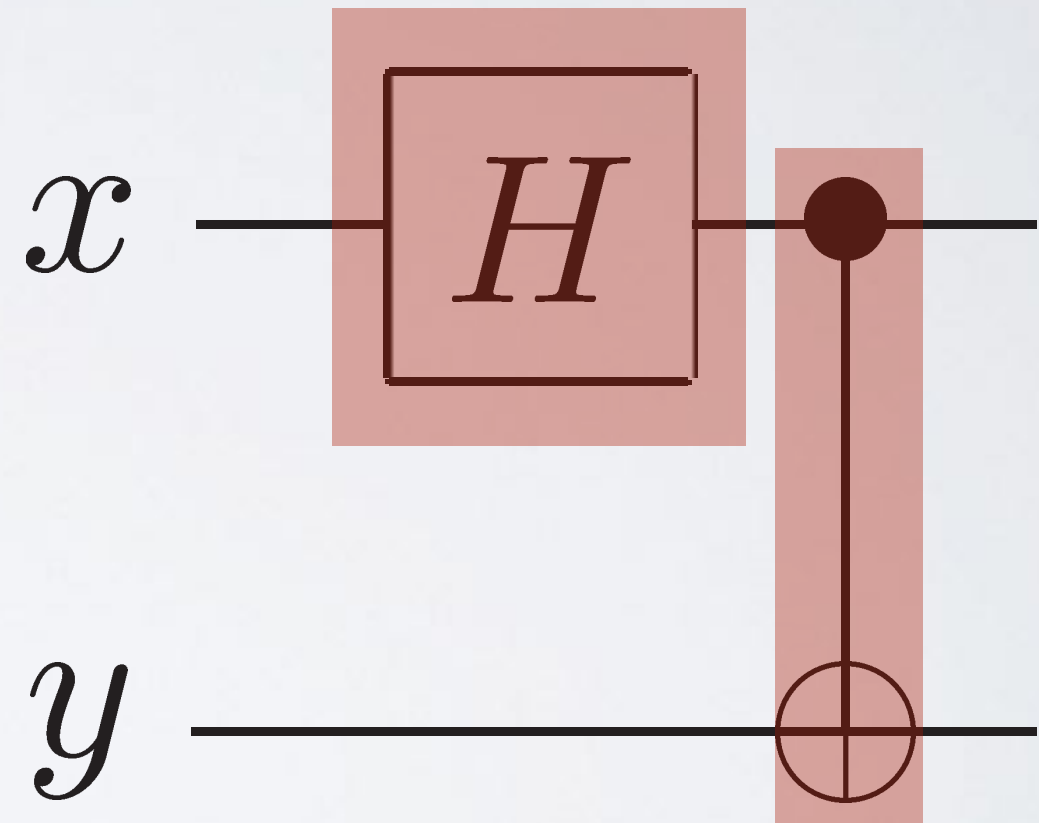
PROGRAMME QUANTIQUE

- Un enchainement de porte quantiques.
- Peut être représenté graphiquement.
 - Plus facile quand on a plusieurs QBits.
- Exemple : obtention d'un *Etat de Bell* :



PROGRAMME QUANTIQUE

- Un enchainement de porte quantiques.
- Peut être représenté graphiquement.
 - Plus facile quand on a plusieurs QBits.
- Exemple : obtention d'un *Etat de Bell* :



PROGRAMME QUANTIQUE

PROGRAMME QUANTIQUE

- Exemple avec en $|00\rangle$ *input* :

PROGRAMME QUANTIQUE

- Exemple avec en $|00\rangle$ *input* :
 - Application de H sur le premier Qbit :

PROGRAMME QUANTIQUE

- Exemple avec en $|00\rangle$ *input* :
 - Application de H sur le premier Qbit :

$$\bullet \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \cdot |0\rangle \Leftrightarrow \frac{(|00\rangle + |10\rangle)}{\sqrt{2}}$$

PROGRAMME QUANTIQUE

- Exemple avec en $|00\rangle$ *input* :
 - Application de H sur le premier Qbit :

$$\bullet \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \cdot |0\rangle \Leftrightarrow \frac{(|00\rangle + |10\rangle)}{\sqrt{2}}$$

- CNOT sur le résultat :

PROGRAMME QUANTIQUE

- Exemple avec en $|00\rangle$ *input* :

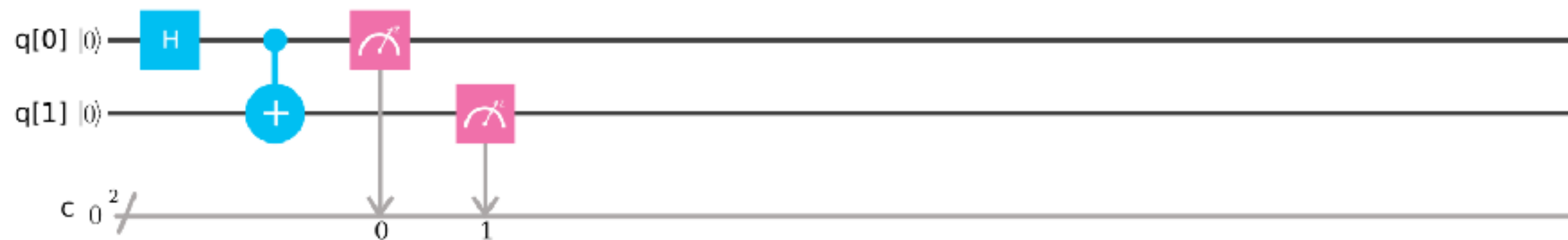
- Application de H sur le premier Qbit :

$$\bullet \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \cdot |0\rangle \Leftrightarrow \frac{(|00\rangle + |10\rangle)}{\sqrt{2}}$$

- CNOT sur le résultat :

$$\bullet \frac{(|00\rangle + |11\rangle)}{\sqrt{2}}$$

PROGRAMME QUANTIQUE



IMPLEMENTATION AVEC QISKIT

PLAN

- Quelques concepts de physique quantique.
- QBits, portes quantiques et programmation.
- Les algorithmes classiques.
- Les principaux acteurs industriels.
- Perspectives

ALGORITHMES CLASSIQUES

ALGORITHMES CLASSIQUES

- Parallélisme quantique

ALGORITHMES CLASSIQUES

- Parallélisme quantique
 - Evaluation d'une fonction en plusieurs points simultanément.

ALGORITHMES CLASSIQUES

- Parallélisme quantique
 - Evaluation d'une fonction en plusieurs points simultanément.
- Recherche quantique

ALGORITHMES CLASSIQUES

- Parallélisme quantique
 - Evaluation d'une fonction en plusieurs points simultanément.
- Recherche quantique
 - Recherche d'un élément dans un tableau non trié (algorithme de Grover).

ALGORITHMES CLASSIQUES

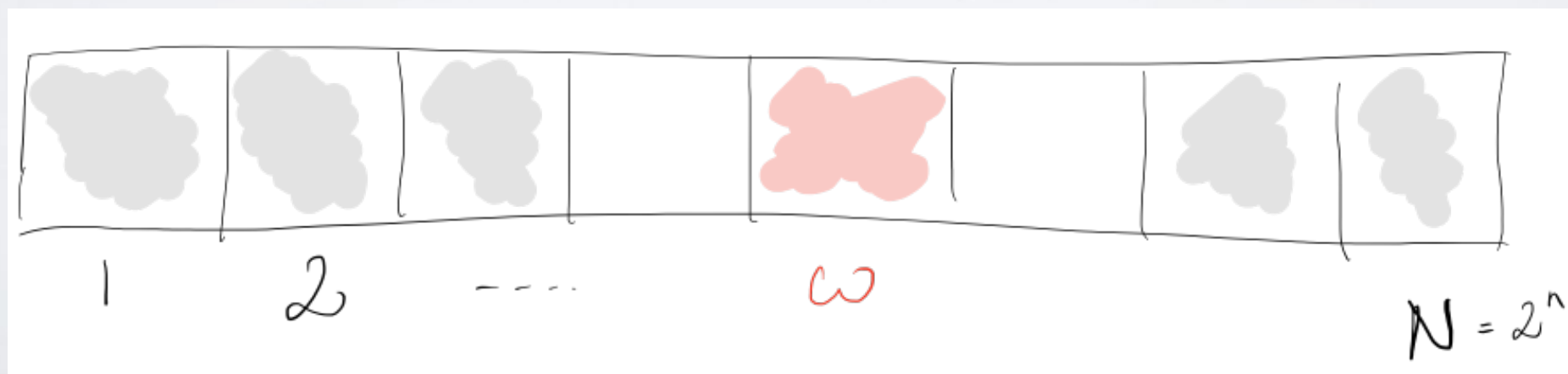
- Parallélisme quantique
 - Evaluation d'une fonction en plusieurs points simultanément.
- Recherche quantique
 - Recherche d'un élément dans un tableau non trié (algorithme de Grover).
- Transformée de Fourier quantique.

ALGORITHMES CLASSIQUES

- Parallélisme quantique
 - Evaluation d'une fonction en plusieurs points simultanément.
- Recherche quantique
 - Recherche d'un élément dans un tableau non trié (algorithme de Grover).
- Transformée de Fourier quantique.
 - Décomposition en facteurs premiers (algorithme de Shor).

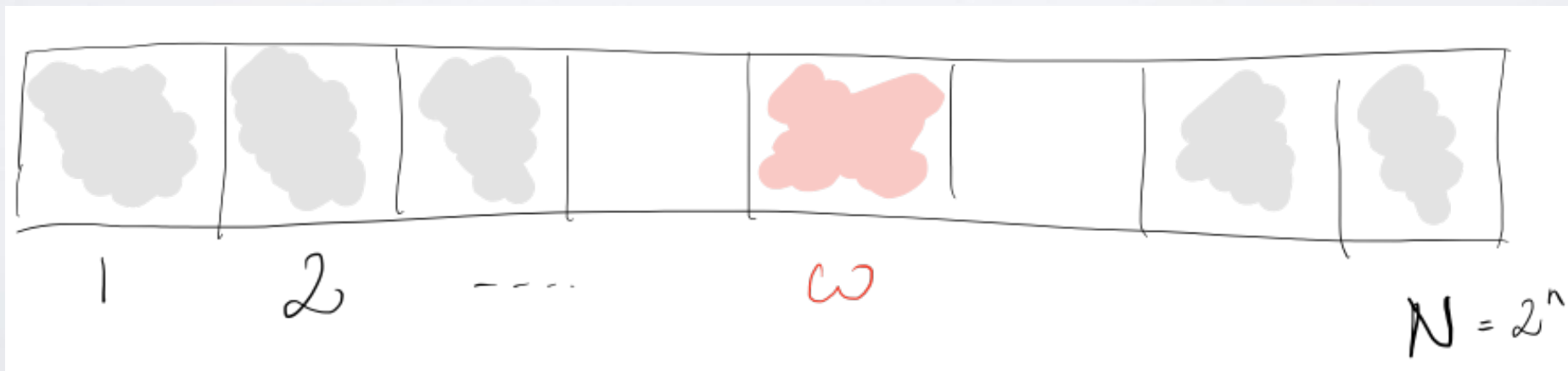
ALGORITHME DE GROVER

- Recherche d'un élément dans un tableau non trié, non structuré de N éléments.
- En informatique classique : en moyenne $N/2$ itérations, au pire N
- En informatique quantique : $\sqrt{N}$



Source : [QisKit.org](https://qiskit.org)

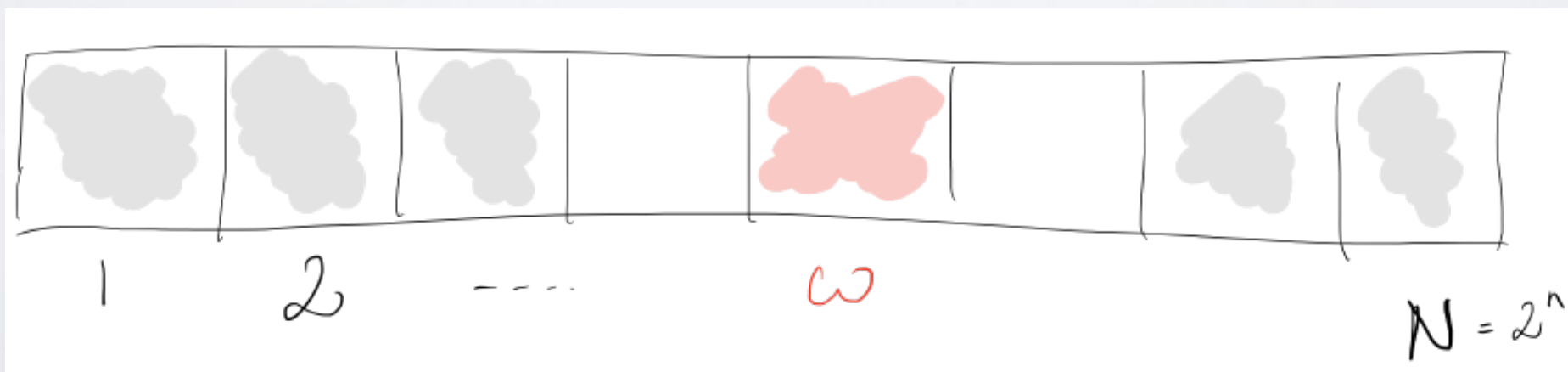
ALGORITHME DE GROVER



Source : [QisKit.org](https://qiskit.org)

ALGORITHME DE GROVER

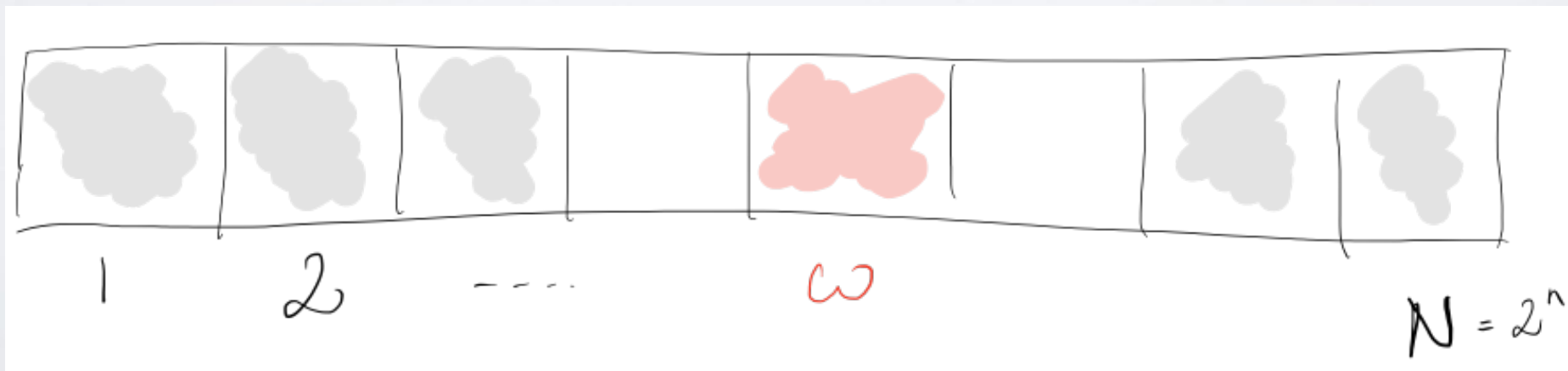
- Principe : utiliser un système $|x\rangle$ à n Qbits avec $2^n = N$.



Source : [QisKit.org](https://qiskit.org)

ALGORITHME DE GROVER

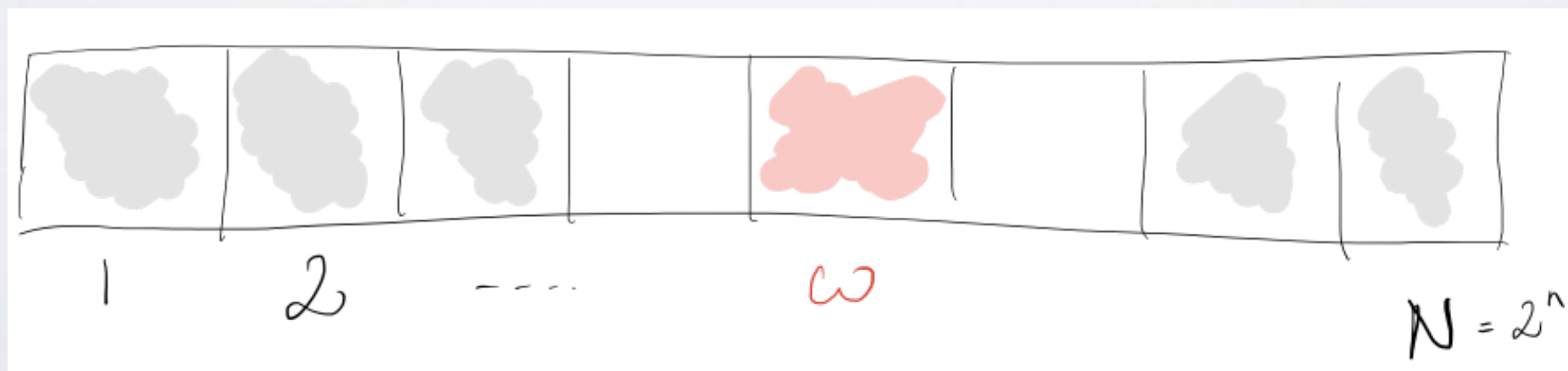
- Principe : utiliser un système $|x\rangle$ à n Qbits avec $2^n = N$.
- L'indice ω de l'élément recherché est compris entre 0 et $2^n - 1$.



Source : [QisKit.org](https://qiskit.org)

ALGORITHME DE GROVER

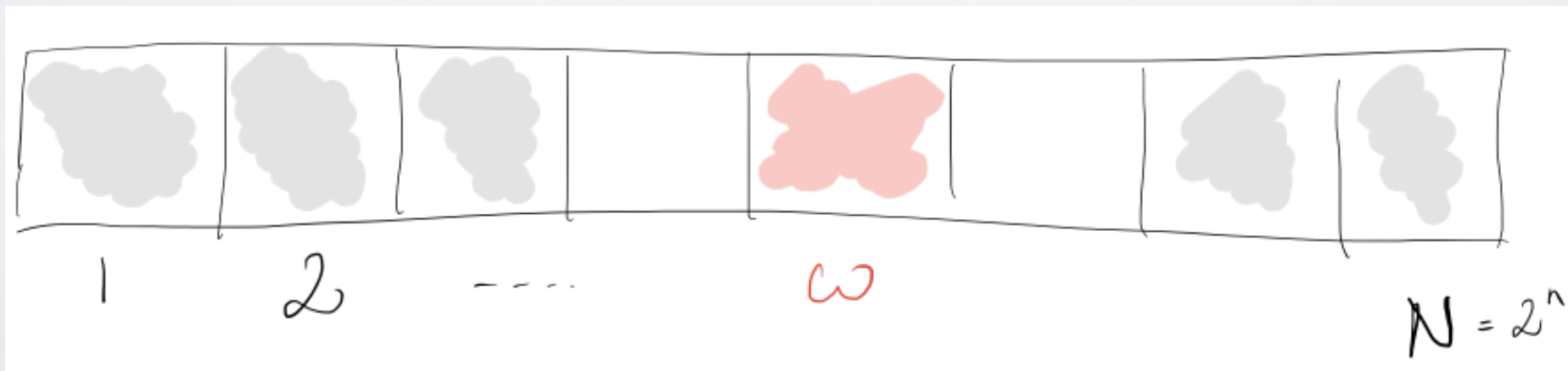
- Principe : utiliser un système $|x\rangle$ à n Qbits avec $2^n = N$.
- L'indice ω de l'élément recherché est compris entre 0 et $2^n - 1$.
- $\Rightarrow |\omega\rangle$ est un des vecteurs de la base sur laquelle se décompose $|x\rangle$.



Source : [QisKit.org](https://qiskit.org)

ALGORITHME DE GROVER

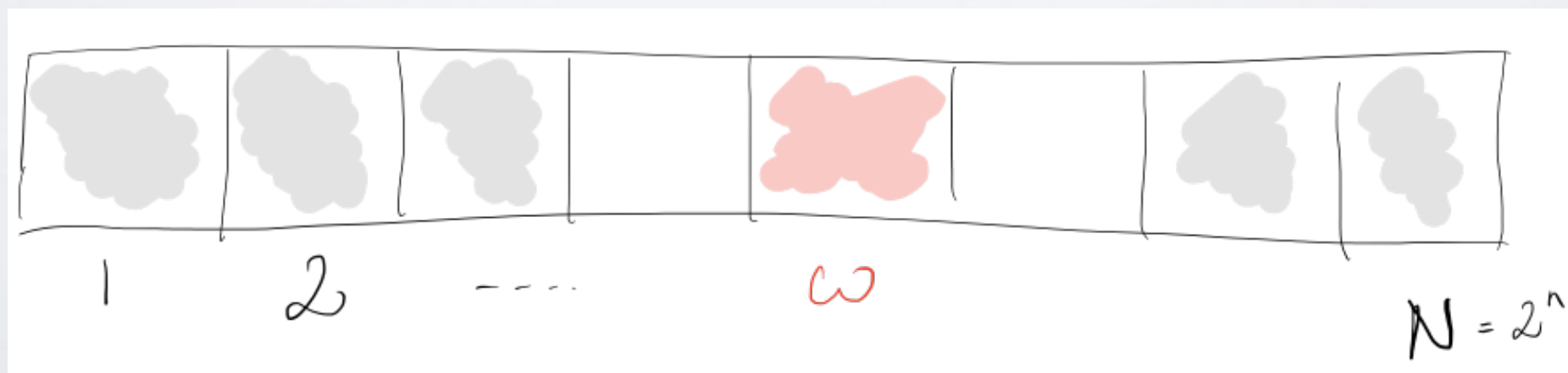
- Principe : utiliser un système $|x\rangle$ à n Qbits avec $2^n = N$.
 - L'indice ω de l'élément recherché est compris entre 0 et $2^n - 1$.
 - $\Rightarrow |\omega\rangle$ est un des vecteurs de la base sur laquelle se décompose $|x\rangle$.
 - Idée : itérer un traitement pour augmenter l'amplitude du vecteur $|\omega\rangle$



Source : [QisKit.org](https://qiskit.org)

ALGORITHME DE GROVER

- Principe : utiliser un système $|x\rangle$ à n Qbits avec $2^n = N$.
 - L'indice ω de l'élément recherché est compris entre 0 et $2^n - 1$.
 - $\Rightarrow | \omega \rangle$ est un des vecteurs de la base sur laquelle se décompose $|x\rangle$.
 - Idée : itérer un traitement pour augmenter l'amplitude du vecteur $| \omega \rangle$
 - $\Rightarrow$ Lors de la mesure : $| \omega \rangle$ aura une probabilité plus élevée que les autres.



Source : [QisKit.org](https://qiskit.org)

ALGORITHME DE GROVER

ALGORITHME DE GROVER

- Encodage : $x \in \{0,1\}^n$ avec $2^n = N$

ALGORITHME DE GROVER

- Encodage : $x \in \{0,1\}^n$ avec $2^n = N$
- Oracle : $f(i) = 1$ si $i = \omega$, 0 sinon.

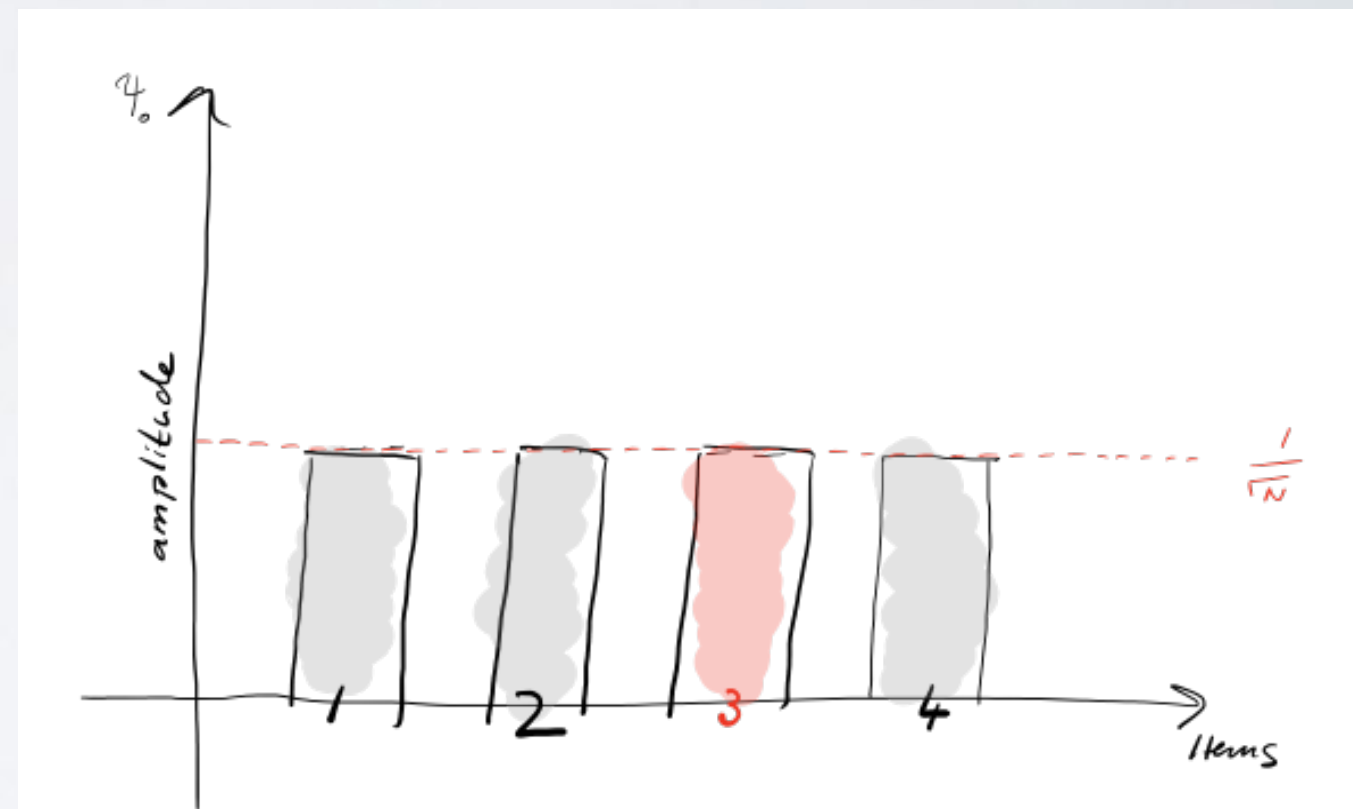
ALGORITHME DE GROVER

- Encodage : $x \in \{0,1\}^n$ avec $2^n = N$
- Oracle : $f(i) = 1$ si $i = \omega$, 0 sinon.
- Matrice oracle : $U_f |i\rangle = (-1)^{f(i)} |i\rangle$

COMMENT ?

- On part de l'état équiprobable :

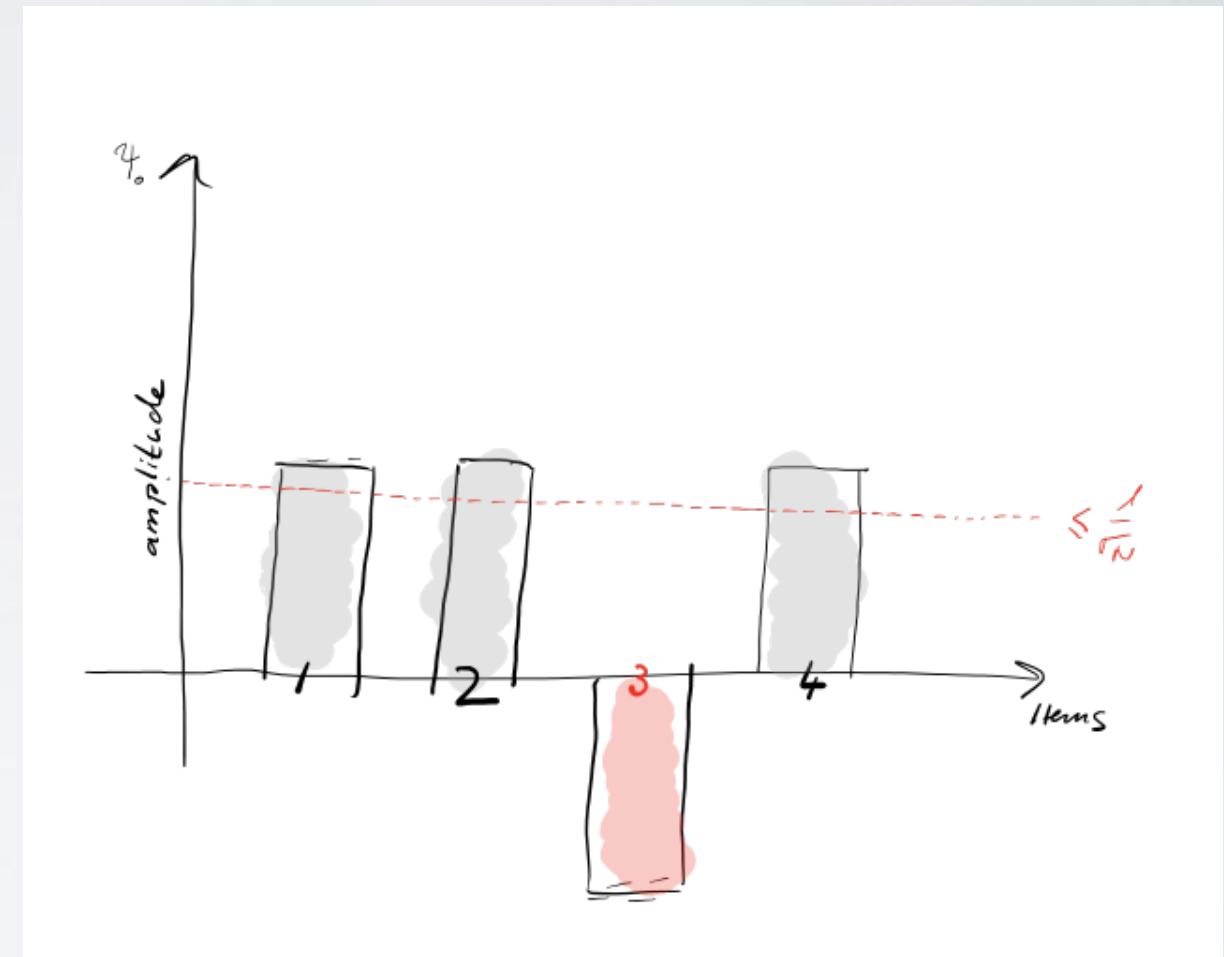
$$|x_0\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle$$



Source : [Qiskit.org](https://qiskit.org)

COMMENT ?

- On applique la réflexion de l'oracle :
- $U_f |x_0\rangle = |x'\rangle$



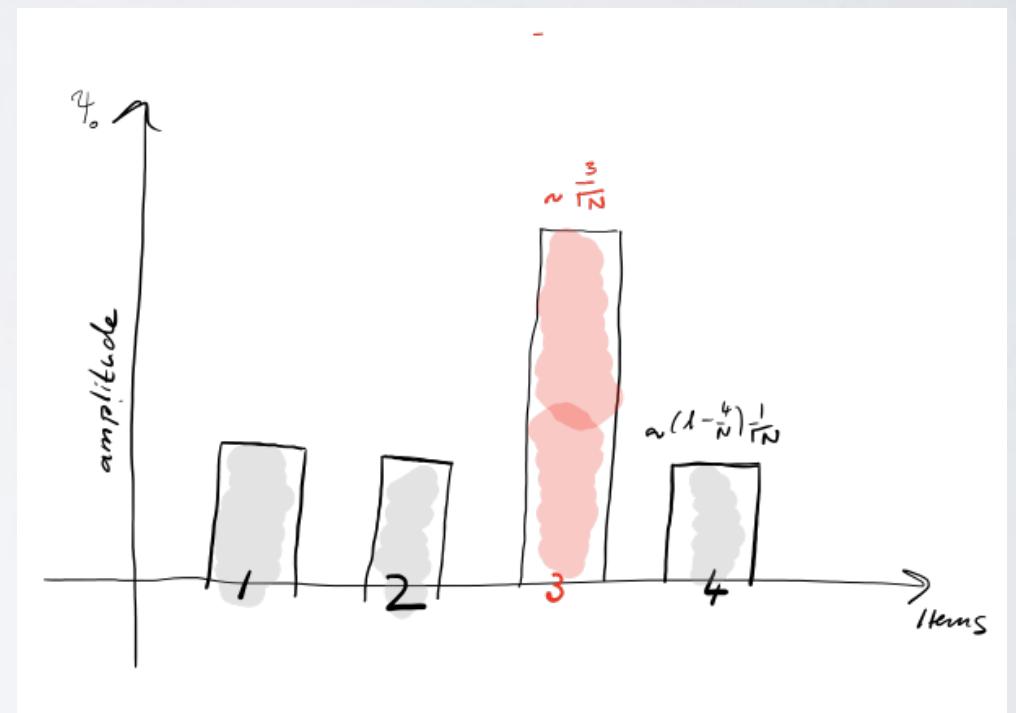
COMMENT ?

- On définit un opérateur réflexif U_x de la manière suivante :

- $U_x = 2|x\rangle\langle x| - 1$

- $U_{x_0}|x'\rangle = |x_1\rangle$

- Et on itère...



COMMENT ?

- Au global :
- $|x_t\rangle = (U_x U_f)^t |x_0\rangle$
- En moyenne, au bout de $\sqrt{N}$ itérations, la mesure donne le bon résultat.

SÉRIEUSEMENT ?

SÉRIEUSEMENT ?

- Oui, détail de l'itération 1:

SÉRIEUSEMENT ?

- Oui, détail de l'itération 1:
- On part de l'état équiprobable :

SÉRIEUSEMENT ?

- Oui, détail de l'itération 1:
- On part de l'état équiprobable :

$$|x_0\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^N |i\rangle$$

SÉRIEUSEMENT ?

- Oui, détail de l'itération 1 :
- On part de l'état équiprobable :

$$• \quad |x_0\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^N |i\rangle$$

- On applique la réflexion U_f :

SÉRIEUSEMENT ?

- Oui, détail de l'itération 1 :
- On part de l'état équiprobable :

$$\bullet \quad |x_0\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^N |i\rangle$$

- On applique la réflexion U_f :

$$\bullet \quad U_f |x_0\rangle = |x'\rangle = |x_0\rangle - \frac{2}{\sqrt{N}} |\omega\rangle$$

SÉRIEUSEMENT ?

SÉRIEUSEMENT ?

- On applique l'opérateur $U_{x_0} : 2|x_0\rangle\langle x_0| - 1$ sur $|x'\rangle$:

SÉRIEUSEMENT ?

- On applique l'opérateur $U_{x_0} : 2|x_0\rangle\langle x_0| - 1$ sur $|x'\rangle$:
 - $U_{x_0}|x'\rangle = 2|x_0\rangle\langle x_0|x'\rangle - |x'\rangle$

SÉRIEUSEMENT ?

- On applique l'opérateur $U_{x_0} : 2|x_0\rangle\langle x_0| - 1$ sur $|x'\rangle$:
 - $U_{x_0}|x'\rangle = 2|x_0\rangle\langle x_0|x'\rangle - |x'\rangle$
- On développe en injectant la valeur de $|x'\rangle$: $|x'\rangle = |x_0\rangle - \frac{2}{\sqrt{N}}|\omega\rangle$

SÉRIEUSEMENT ?

- On applique l'opérateur $U_{x_0} : 2|x_0\rangle\langle x_0| - 1$ sur $|x'\rangle$:

- $U_{x_0}|x'\rangle = 2|x_0\rangle\langle x_0|x'\rangle - |x'\rangle$

- On développe en injectant la valeur de $|x'\rangle$: $|x'\rangle = |x_0\rangle - \frac{2}{\sqrt{N}}|\omega\rangle$

- $= 2|x_0\rangle\langle x_0|x_0\rangle - \frac{4}{\sqrt{N}}|x_0\rangle\langle x_0|\omega\rangle - |x_0\rangle + \frac{2}{\sqrt{N}}|\omega\rangle$

SÉRIEUSEMENT ?

- On applique l'opérateur $U_{x_0} : 2|x_0\rangle\langle x_0| - 1$ sur $|x'\rangle$:

- $U_{x_0}|x'\rangle = 2|x_0\rangle\langle x_0|x'\rangle - |x'\rangle$

- On développe en injectant la valeur de $|x'\rangle$: $|x'\rangle = |x_0\rangle - \frac{2}{\sqrt{N}}|\omega\rangle$

- $= 2|x_0\rangle\langle x_0|x_0\rangle - \frac{4}{\sqrt{N}}|x_0\rangle\langle x_0|\omega\rangle - |x_0\rangle + \frac{2}{\sqrt{N}}|\omega\rangle$

- $= \frac{N-4}{N}|x_0\rangle + \frac{2}{\sqrt{N}}|\omega\rangle$

SÉRIEUSEMENT ?

- On applique l'opérateur $U_{x_0} : 2|x_0\rangle\langle x_0| - 1$ sur $|x'\rangle$:

- $U_{x_0}|x'\rangle = 2|x_0\rangle\langle x_0|x'\rangle - |x'\rangle$

- On développe en injectant la valeur de $|x'\rangle$: $|x'\rangle = |x_0\rangle - \frac{2}{\sqrt{N}}|\omega\rangle$

- $= 2|x_0\rangle\langle x_0|x_0\rangle - \frac{4}{\sqrt{N}}|x_0\rangle\langle x_0|\omega\rangle - |x_0\rangle + \frac{2}{\sqrt{N}}|\omega\rangle$

- $= \frac{N-4}{N}|x_0\rangle + \frac{2}{\sqrt{N}}|\omega\rangle$

DISCUSSION

DISCUSSION

- Ça marche en vrai ?

DISCUSSION

- Ça marche en vrai ?
- Réponse courte : non.

DISCUSSION

- Ça marche en vrai ?
- Réponse courte : non.
- Réponse longue :

DISCUSSION

- Ça marche en vrai ?
- Réponse courte : non.
- Réponse longue :
 - Problème de l'implémentation de $f(x)$.

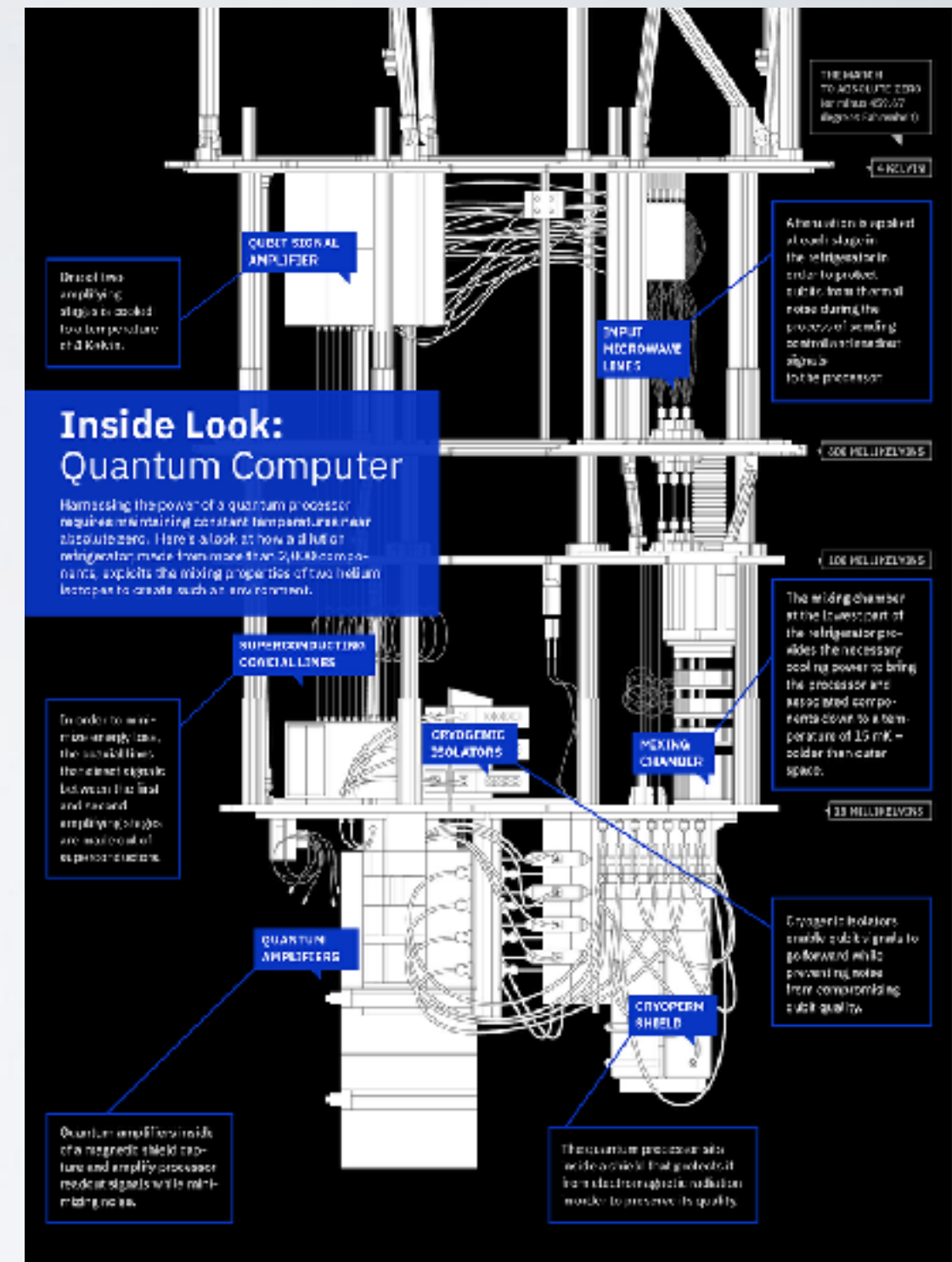
PLAN

- Quelques concepts de la physique quantique.
- QBits, portes quantiques et programmation.
- Les algorithmes classiques.
- Les principaux acteurs industriels.
- Perspectives

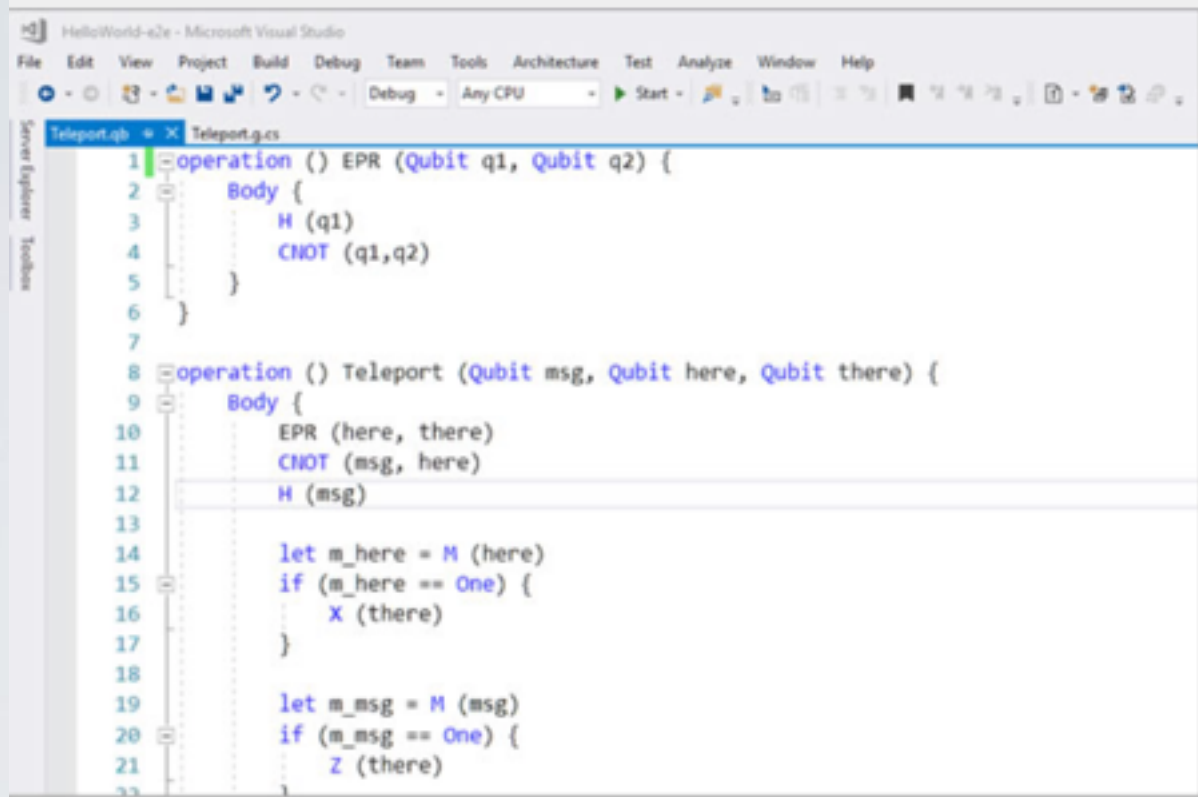
IBM QUANTUM PROJECT



Qiskit



MICROSOFT

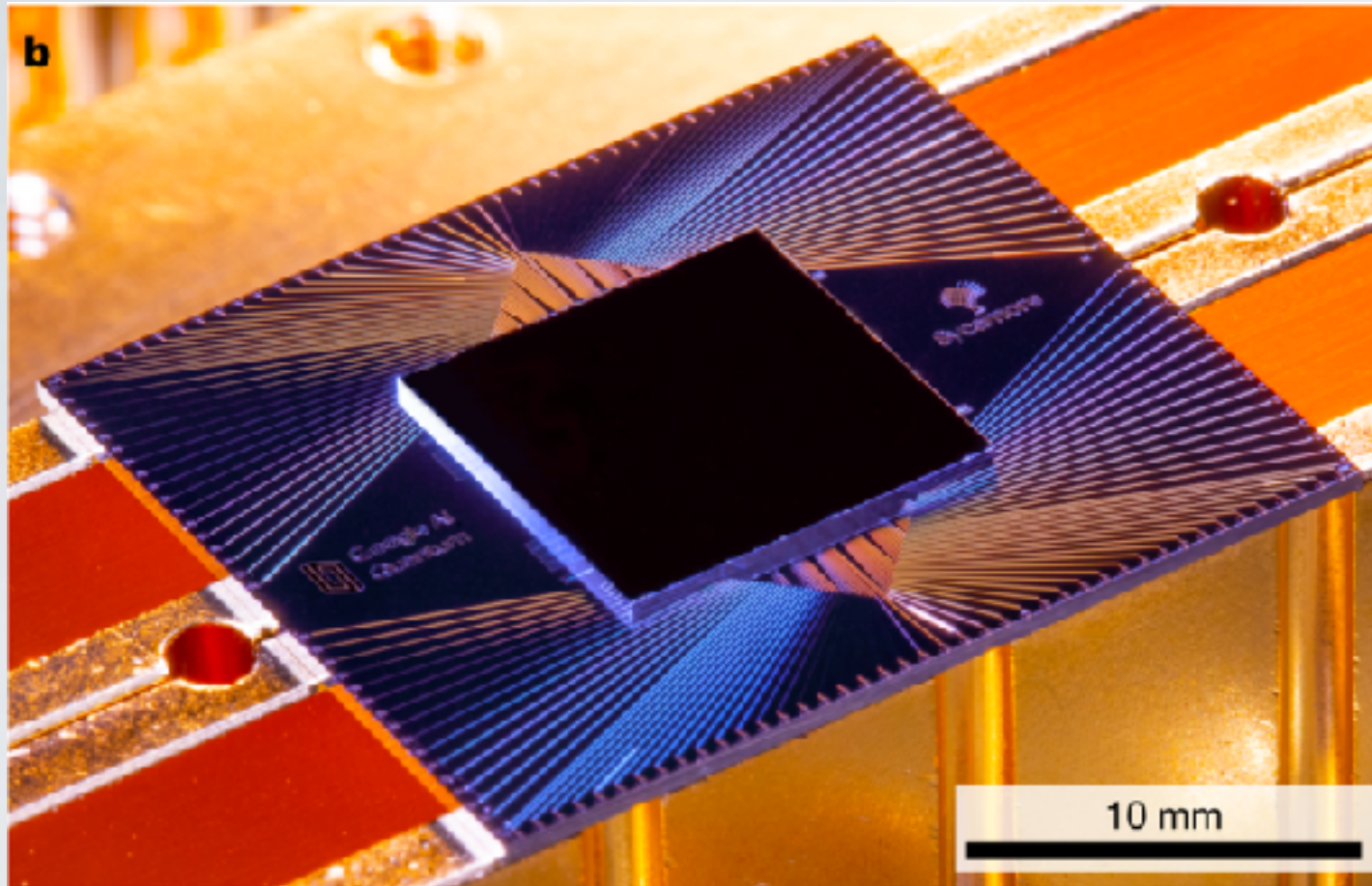


The image shows a screenshot of the Microsoft Visual Studio IDE. The main window displays a Q# script named `Teleport.qs`. The code defines two operations: `EPR` and `Teleport`. The `EPR` operation takes two qubits, `q1` and `q2`, and applies an `H` gate to `q1` followed by a `CNOT` gate with `q1` as the control and `q2` as the target. The `Teleport` operation takes three qubits: `msg`, `here`, and `there`. It first calls the `EPR` operation on `here` and `there`, then applies a `CNOT` gate with `msg` as the control and `here` as the target, followed by an `H` gate on `msg`. Finally, it performs two measurements: `M` on `here` and `M` on `msg`. Based on the results of these measurements, it applies `X` and `Z` gates to `there` to complete the teleportation. The Visual Studio interface includes a menu bar (File, Edit, View, Project, Build, Debug, Team, Tools, Architecture, Test, Analyze, Window, Help), a toolbar with icons for running, debugging, and other actions, and a sidebar on the left showing the 'Server Explorer' and 'Toolbox'.

```
1 operation () EPR (Qubit q1, Qubit q2) {  
2     Body {  
3         H (q1)  
4         CNOT (q1,q2)  
5     }  
6 }  
7  
8 operation () Teleport (Qubit msg, Qubit here, Qubit there) {  
9     Body {  
10        EPR (here, there)  
11        CNOT (msg, here)  
12        H (msg)  
13  
14        let m_here = M (here)  
15        if (m_here == One) {  
16            X (there)  
17        }  
18  
19        let m_msg = M (msg)  
20        if (m_msg == One) {  
21            Z (there)  
22        }  
23    }  
24 }
```



GOOGLE



GOOGLE



Quantum A.I.

Quantum Computing merges two great scientific revolutions of the 20th century: computer science and quantum physics. Quantum physics is the theoretical basis of the transistor, the laser, and other technologies which enabled the computing revolution. But on the algorithmic level today's computing machinery still operates on "classical" Boolean logic. Quantum computing is the design of hardware and software that replaces Boolean logic by quantum law at the algorithmic level. For certain computations such as optimization, sampling, search or quantum simulation this promises dramatic speedups. Soon we hope to falsify the strong Church-Turing thesis: we will perform computations which

20 Publications

Bounding the Costs of Quantum Simulation of Many-Body Physics in Real Space



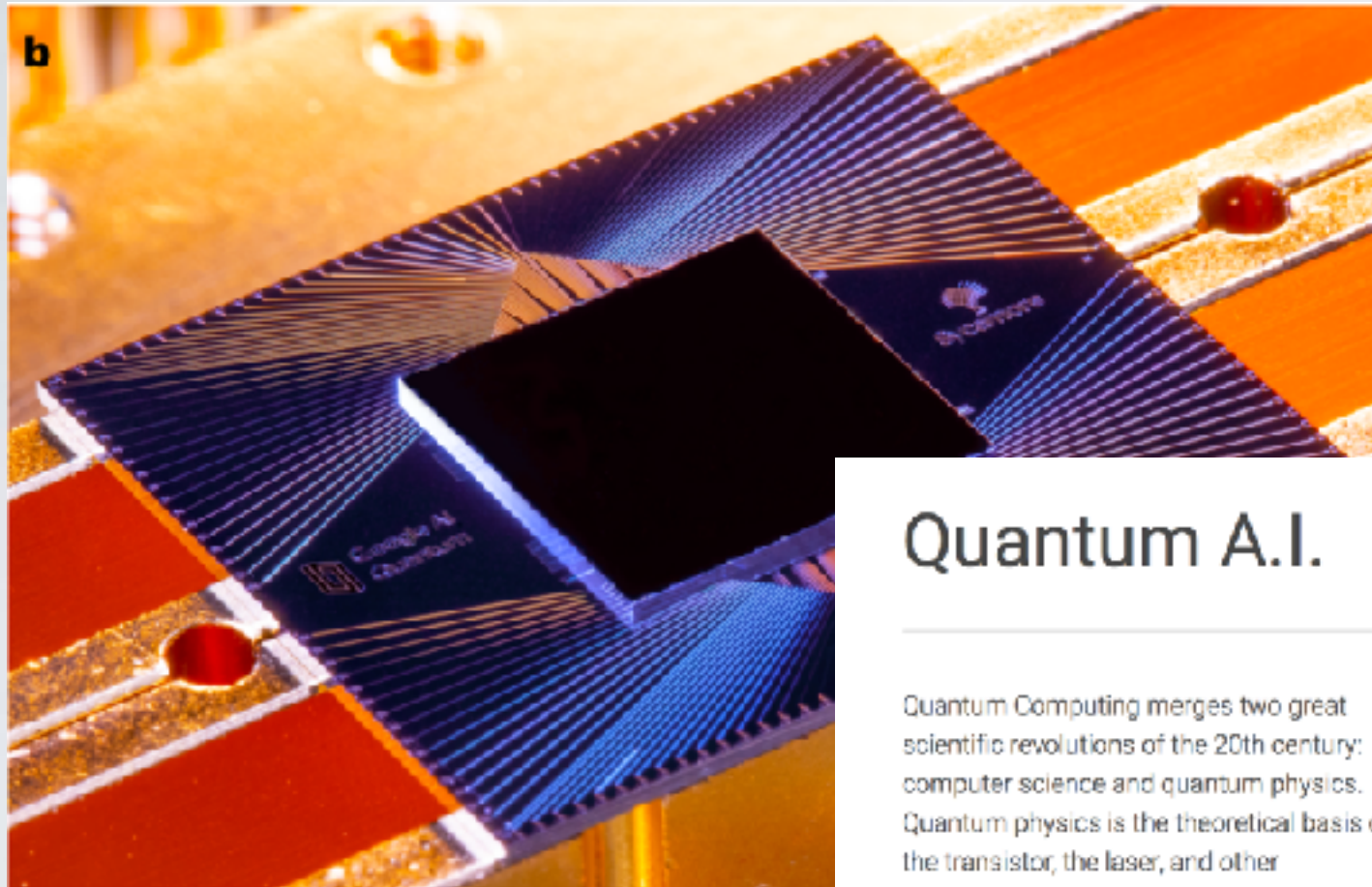
Ian D. Kivlichan, Nathan Wiebe, [Ryan Babbush](#), Alán Aspuru-Guzik
Journal of Physics A: Mathematical and Theoretical, vol. 50 (2017), pp. 305301

Characterizing Quantum Supremacy in Near-Term Devices



[Sergio Boixo](#), Sergei Isakov, Vadim Smelyanskiy, [Ryan Babbush](#), Nan Ding, Zhang Jiang,

GOOGLE



Quantum A.I.

Quantum Computing merges two great scientific revolutions of the 20th century: computer science and quantum physics. Quantum physics is the theoretical basis of the transistor, the laser, and other technologies which enabled the computing revolution. But on the algorithmic level today's computing machinery still operates on "classical" Boolean logic. Quantum computing is the design of hardware and software that replaces Boolean logic by quantum law at the algorithmic level. For certain computations such as optimization, sampling, search or quantum simulation this promises dramatic speedups. Soon we hope to falsify the strong Church-Turing thesis: we will perform computations which

20 Publications

Bounding the Costs of Quantum Simulation of Many-Body Physics in Real Space



Ian D. Kivlichan, Nathan Wiebe, [Ryan Babbush](#), Alán Aspuru-Guzik

Journal of Physics A: Mathematical and Theoretical, vol. 50 (2017), pp. 305301

Characterizing Quantum Supremacy in Near-Term Devices



[Sergio Boixo](#), Sergei Isakov, Vadim Smelyanskiy, [Ryan Babbush](#), Nan Ding, Zhang Jiang,

Article

Quantum supremacy using a programmable superconducting processor

<https://doi.org/10.1038/s41586-019-1666-5>

Received: 22 July 2019

Accepted: 20 September 2019

Published online: 23 October 2019

Frank Arute¹, Kunal Arya¹, Ryan Babbush¹, Dave Bacon¹, Joseph C. Bardin^{1,2}, Rami Barends¹, Rupak Biswas³, Sergio Boixo¹, Fernando G. S. L. Brandao^{1,4}, David A. Buell¹, Brian Burkett¹, Yu Chen¹, Zijun Chen¹, Ben Chiaro⁵, Roberto Collins¹, William Courtney¹, Andrew Dunsworth¹, Edward Farhi¹, Brooks Foxen^{1,5}, Austin Fowler¹, Craig Gidney¹, Marissa Giustina¹, Rob Graff¹, Keith Guerín¹, Steve Habegger¹, Matthew P. Harrigan¹, Michael J. Hartmann^{1,6}, Alan Ho¹, Markus Hoffmann¹, Trent Huang¹, Travis S. Humble⁷, Sergei V. Isakov¹, Evan Jeffrey¹, Zhang Jiang¹, Dvir Kafri¹, Kostyantyn Kechedzhi¹, Julian Kelly¹, Paul V. Klimov¹, Sergey Knysh¹, Alexander Korotkov^{1,8}, Fedor Kostritsa¹, David Landhuis¹, Mike Lindmark¹, Erik Lucero¹, Dmitry Lyakh⁹, Salvatore Mandrà^{3,10}, Jarrod R. McClean¹, Matthew McEwen⁵, Anthony Megrant¹, Xiao Mi¹, Kristel Michielsen^{11,12}, Masoud Mohseni¹, Josh Mutus¹, Ofer Naaman¹, Matthew Neeley¹, Charles Neill¹, Murphy Yuezhen Niu¹, Eric Ostby¹, Andre Petukhov¹, John C. Platt¹, Chris Quintana¹, Eleanor G. Rieffel³, Pedram Roushan¹, Nicholas C. Rubin¹, Daniel Sank¹, Kevin J. Satzinger¹, Vadim Smelyanskiy¹, Kevin J. Sung^{1,13}, Matthew D. Trevithick¹, Amit Vainsencher¹, Benjamin Villalonga^{1,14}, Theodore White¹, Z. Jamie Yao¹, Ping Yeh¹, Adam Zalcman¹, Hartmut Neven¹ & John M. Martinis^{1,5*}

D-WAVE

- Précurseurs ?
- Seul acteur qui commercialise les machines.
- 2000 QBits.
- Est limité à un type de problème.



PLAN

- Quelques concepts de la physique quantique.
- QBits, portes quantiques et programmation.
- Les algorithmes classiques.
- Outils matériels et logiciels
- Perspectives

PERSPECTIVES

- Domaines d'applications multiples :
 - Cryptographie, Machine learning, Chimie, Finances...
- Progrès importants :
 - Record actuel du nb de QBits : Google, avec 54 QBits.
- Mais pour l'instant : utilisabilité très limitée.
 - Bruit omniprésent.
 - NISQ.

PERSPECTIVES

- Applications existantes chez IBM :
 - Résolution de systèmes d'équations linéaires.
 - Simulation de molécules.
 - Optimisation combinatoire.
 - Réseaux neurones hybrides quantiques / classiques.

REFERENCES

- Mécanique Quantique, 2eme édition
 - C. Cohen-Tannoudji, Bernard Diu, Franck Laloe
 - ISBN 2 7056 6121 2
- Quantum computation and quantum information :
 - Michael A. Nielsen and Isaac Chuang,
 - American Journal of Physics 70, 558 (2002); <https://doi.org/10.1119/1.1463744>
- QisKit

MERCI POUR VOTRE ATTENTION

Questions ? Remarques ?

