


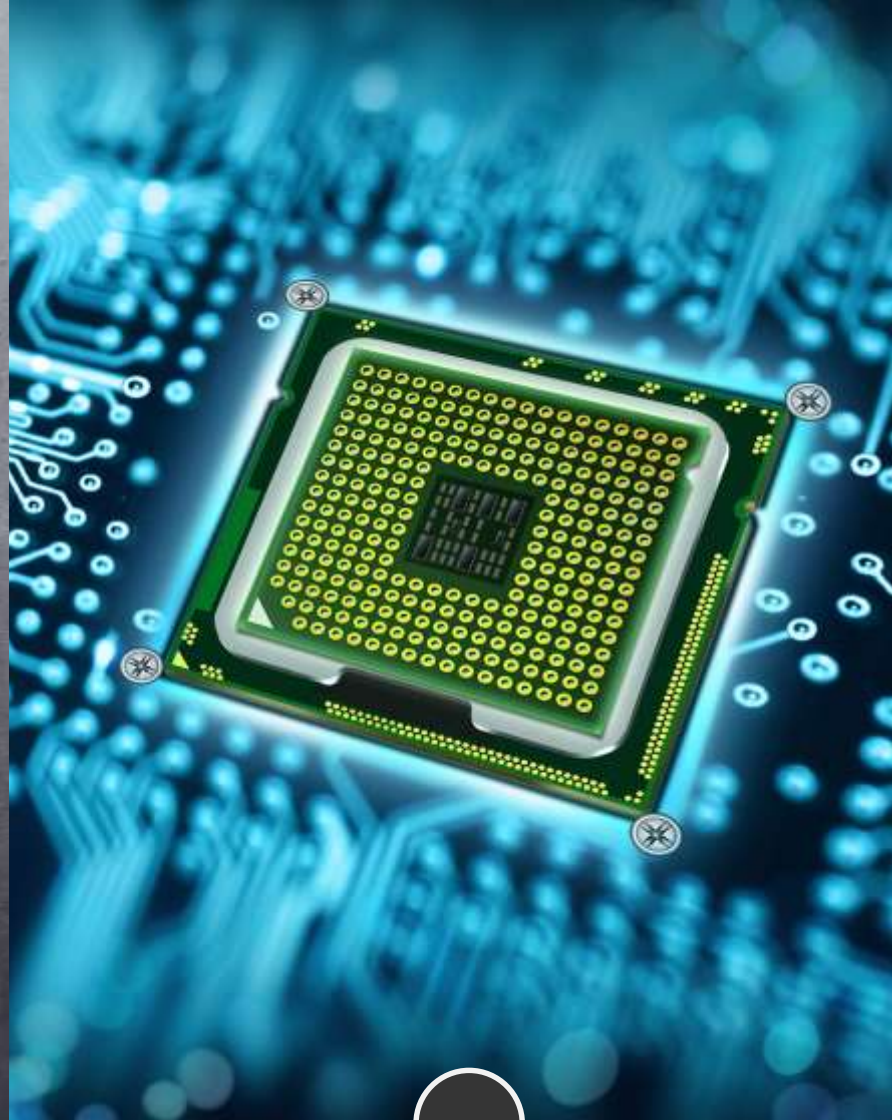
# Bienvenue à l'ère Quantique

Bernard Ourghanlian  
CTO & CSO – Microsoft France  
 @Ourghanlian





2500  
avant JC



20<sup>ème</sup>  
siècle



21<sup>ème</sup>  
siècle



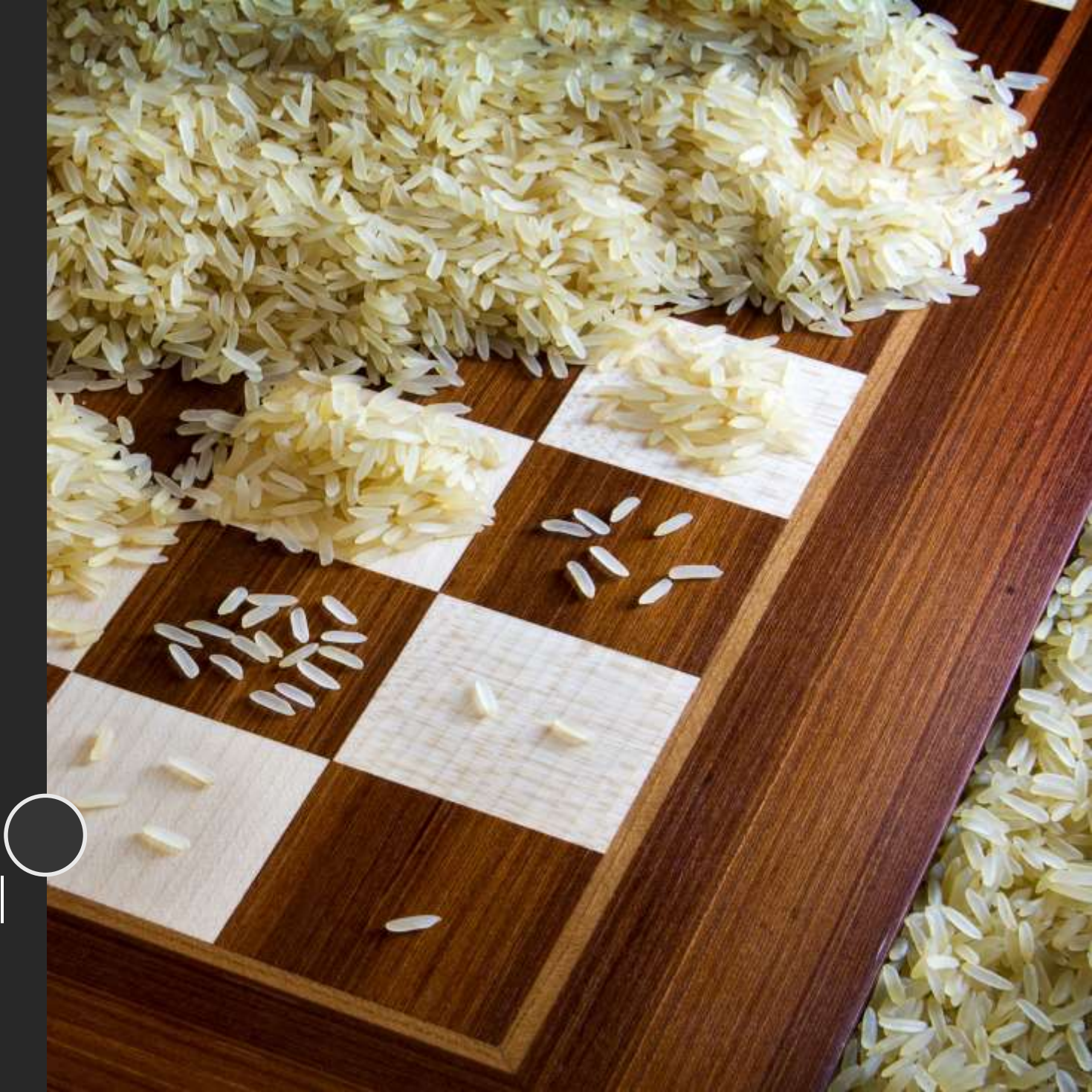


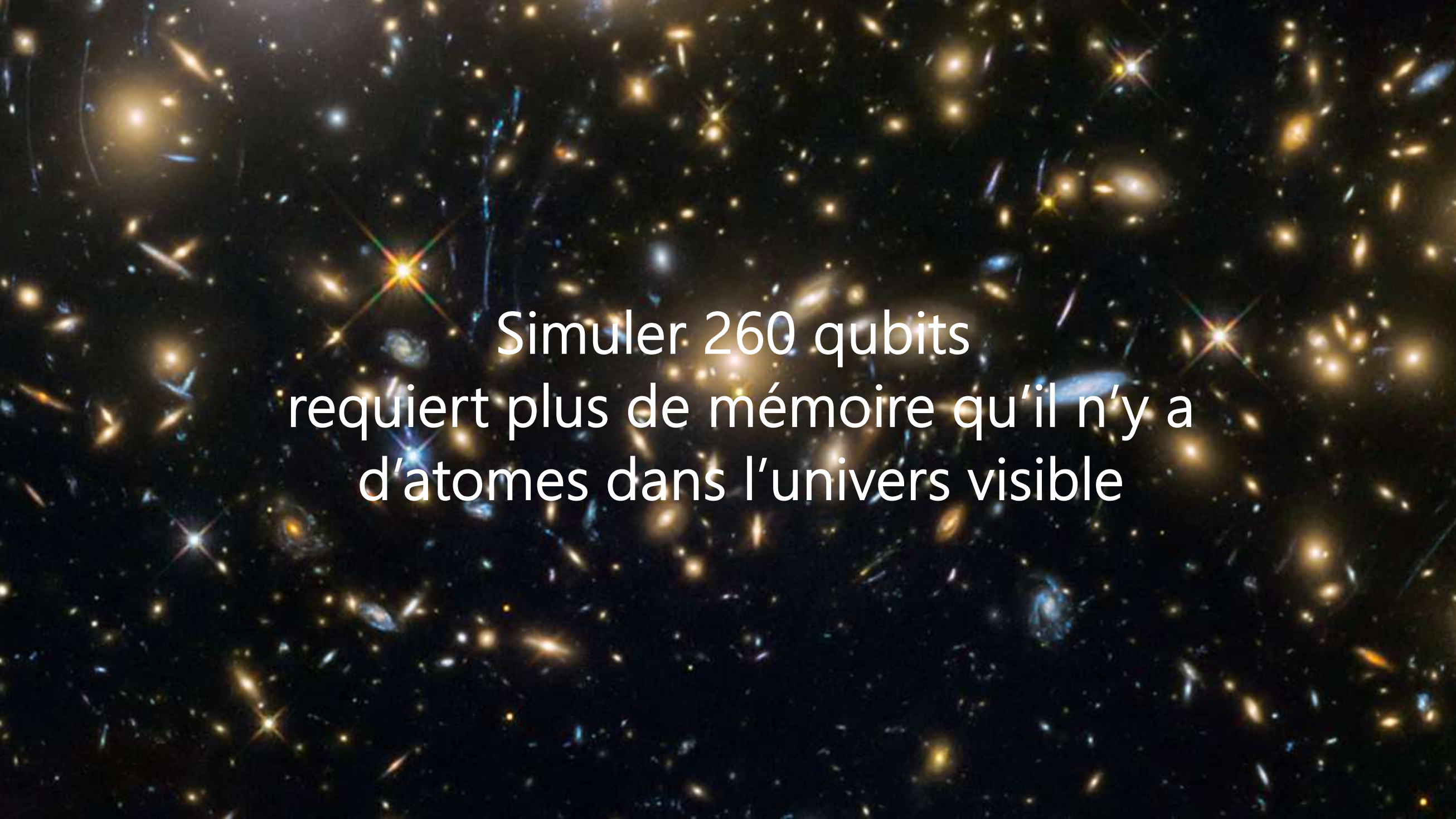
30 qubits → 16 Gb

40 qubits → 16 Tb

50 qubits → 16 Pb

Passage à l'échelle exponentiel





Simuler 260 qubits  
requiert plus de mémoire qu'il n'y a  
d'atomes dans l'univers visible



Quantum 1.0



# FORMALISER LA MECANIQUE QUANTIQUE



Feynman

1982

Feynman a remarqué que les équations de base de la mécanique quantique sont extrêmement difficiles à résoudre...

100 spins (propriétés des particules au même titre que la masse ou la charge – moment cinétique ou magnétique) en interactions requièrent une fonction d'onde à  $2^{100}$  dimensions.

Des systèmes quantiques très simples peuvent avoir une puissance de calcul extraordinaire.

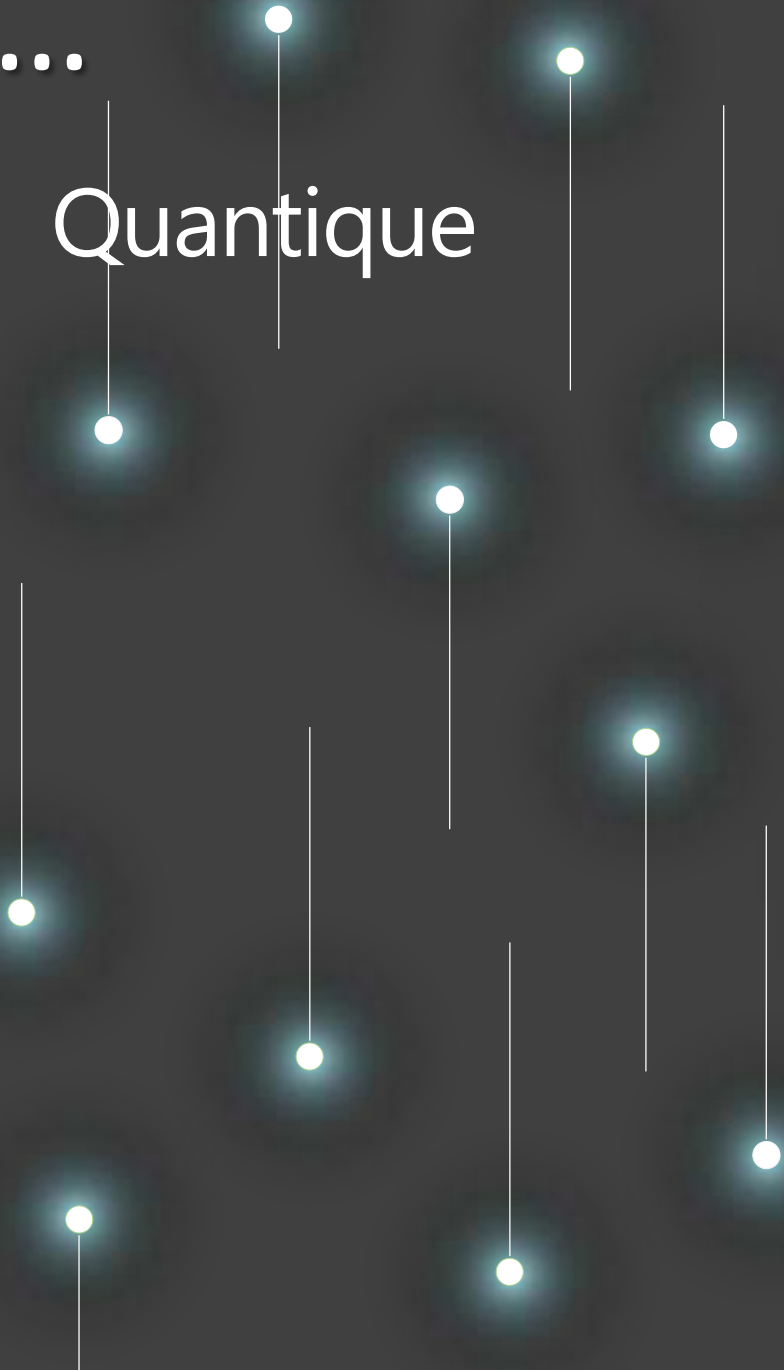
Sa solution : Construire un ordinateur qui a des propriétés quantiques construites directement au sein du système.

# DEUX MONDES DIFFERENTS...

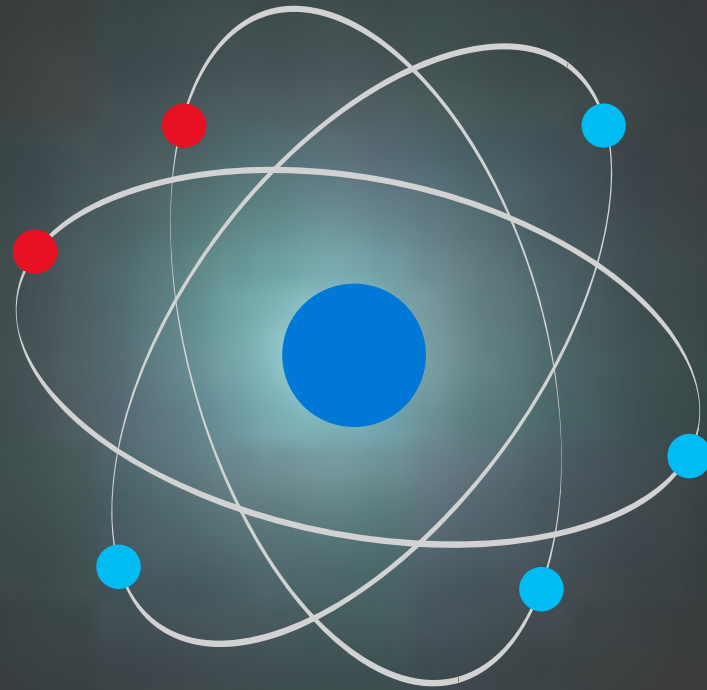
Classique



Quantique



# MECANIQUE QUANTIQUE

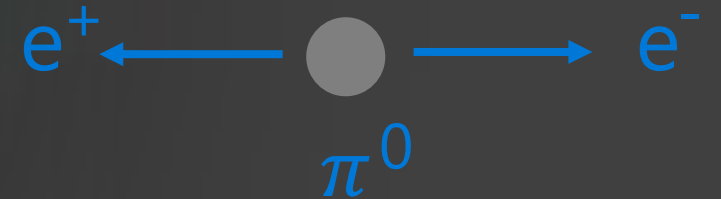


## SUPERPOSITION



un même état quantique  
peut posséder plusieurs valeurs  
pour une certaine quantité observable

## INTRICATION



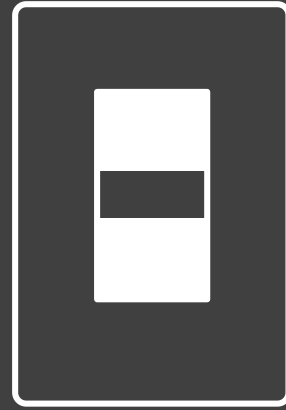
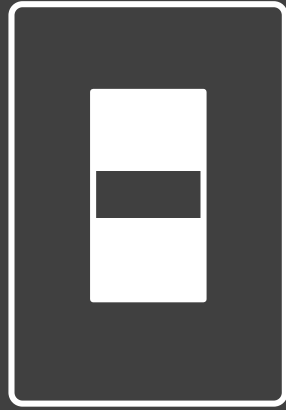
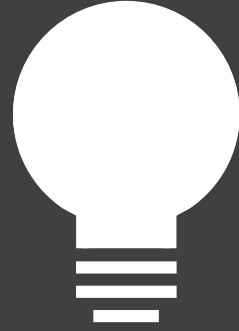
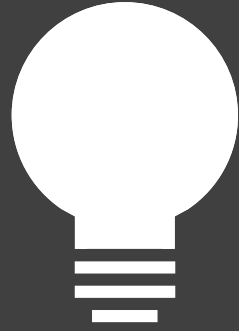
phénomène dans lequel deux particules  
(ou groupes de particules)  
ont des états quantiques dépendant  
l'un de l'autre quelle que soit  
la distance qui les sépare.

# BITS

Classiques

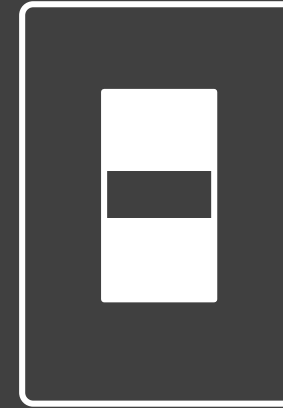
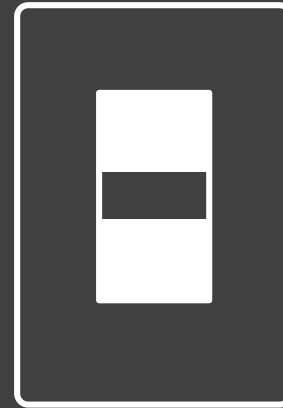
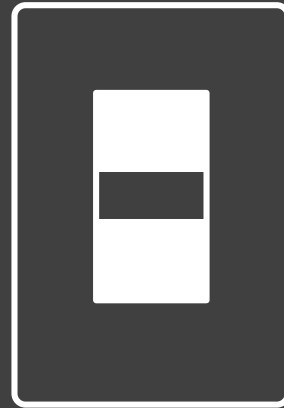
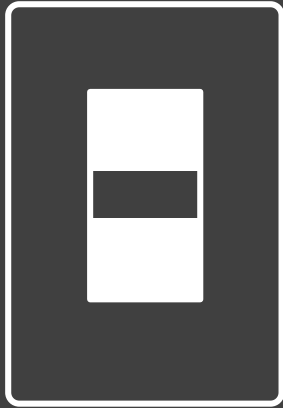
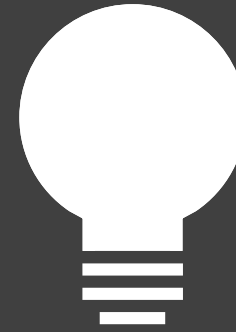
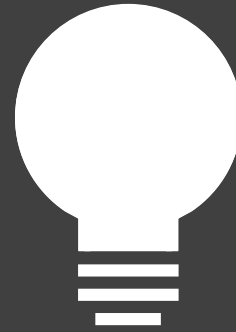
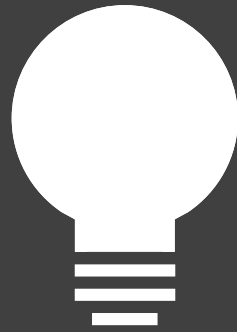
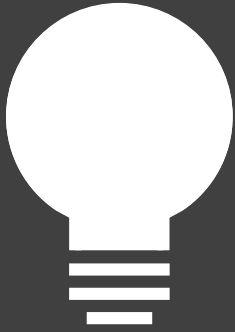
Qubits

01001010000100101100  
10001000000100000001  
10000000100000100000  
10001011010001100010  
10010000100000100001  
100010000100000100001  
10010000100000100001



Ω

Ω



Ω

Ω

Ω

Ω

0000

0001

0010

0011

0100

0101

0110

0111

1000

1001

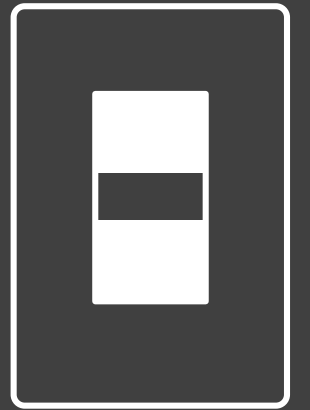
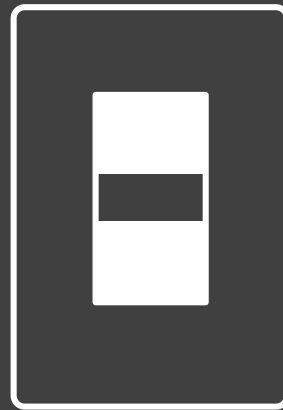
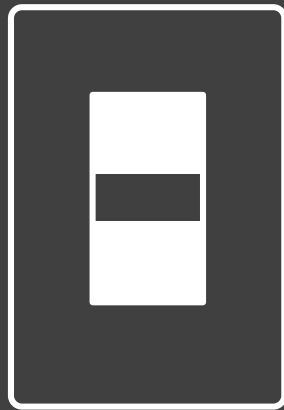
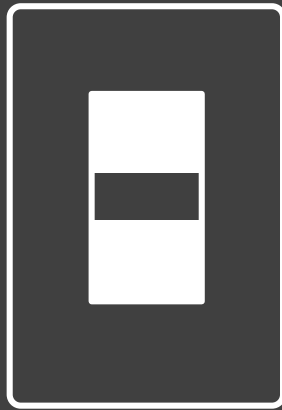
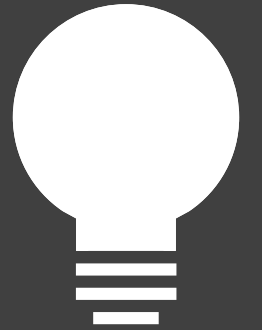
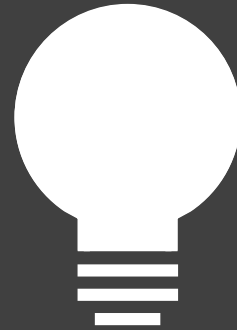
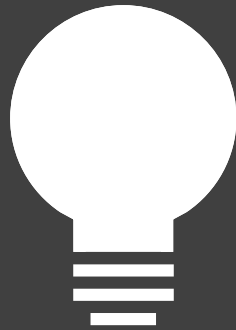
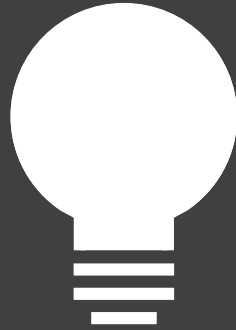
1010

1011

1100

1101

1111









NOT



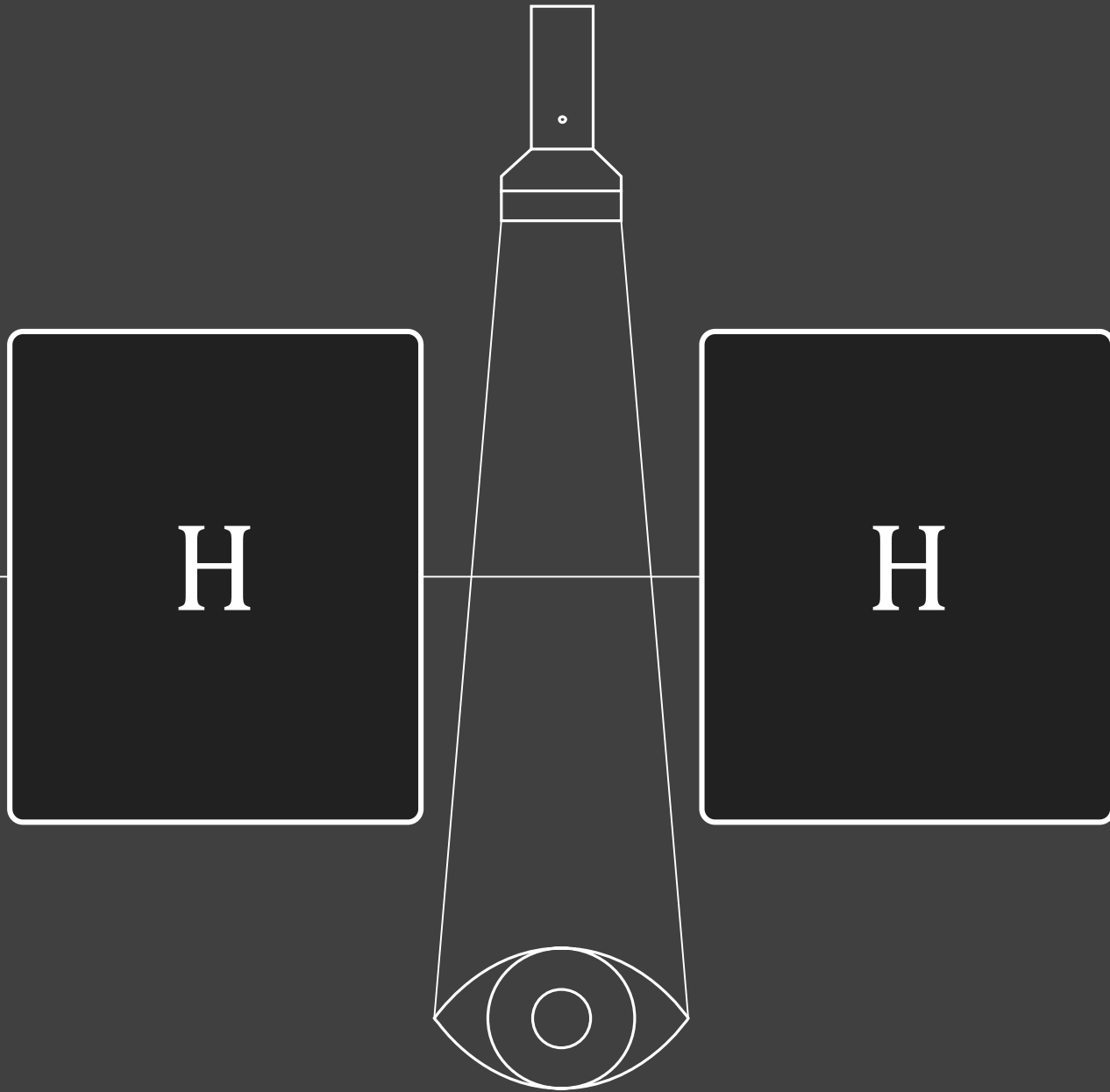
NOT

NOT

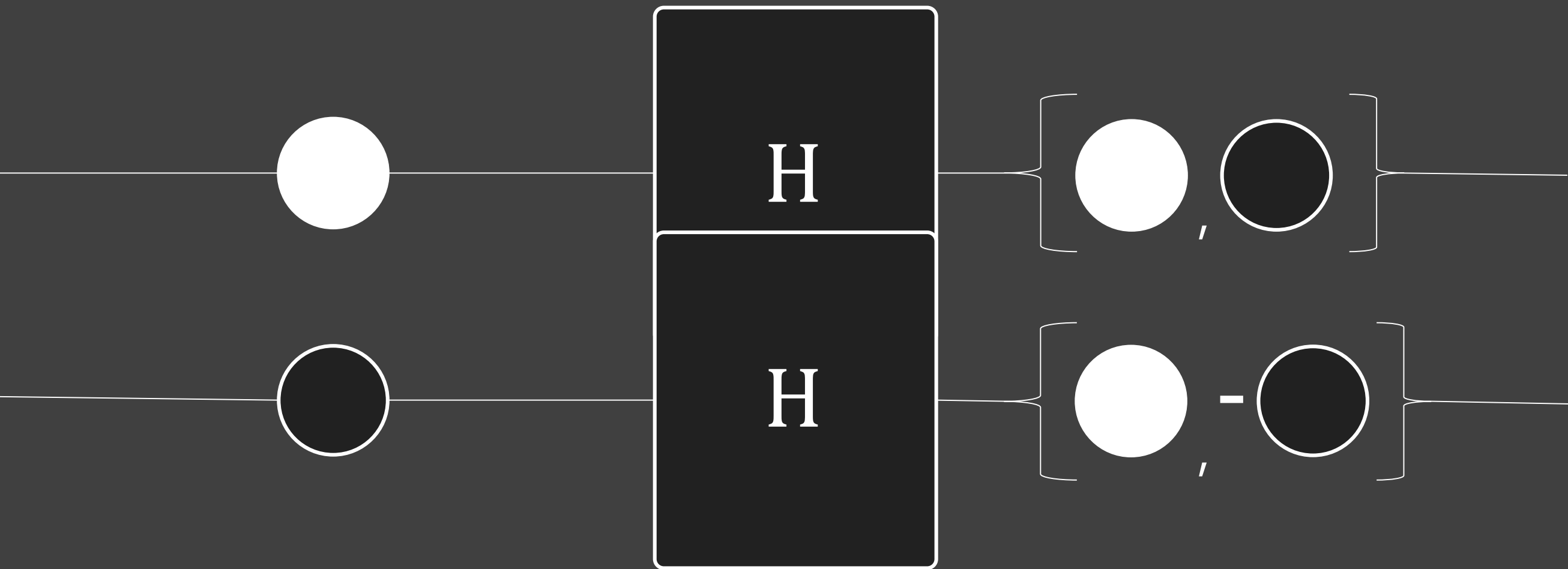


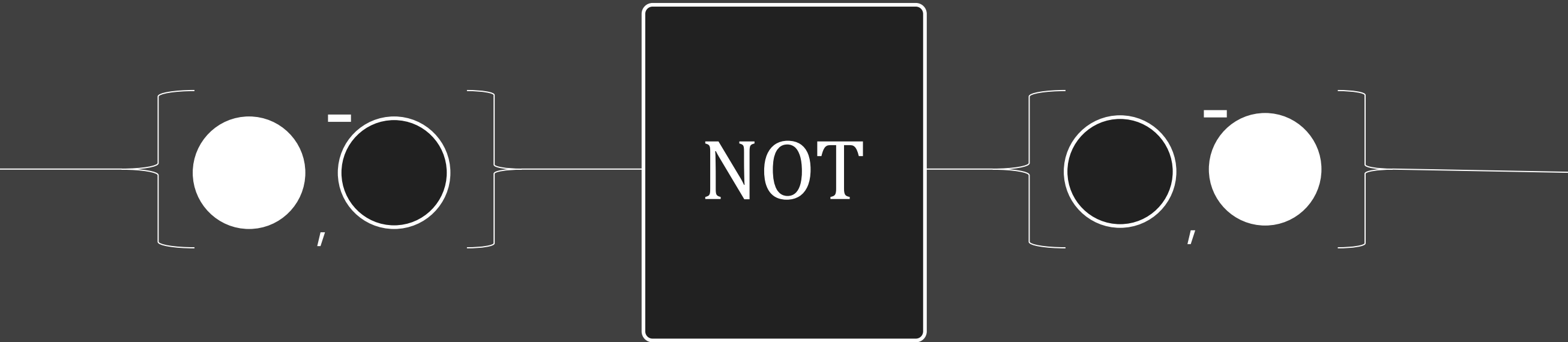
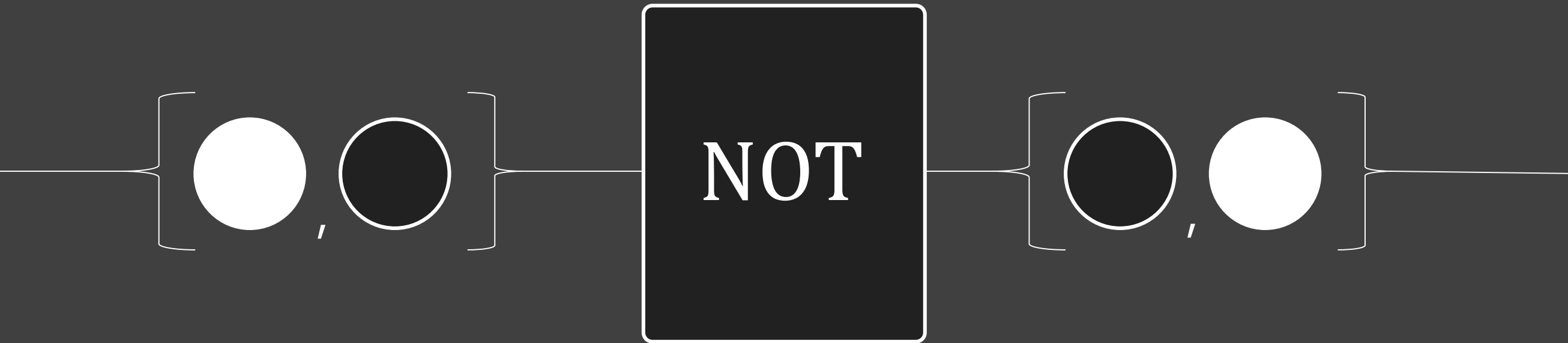
H



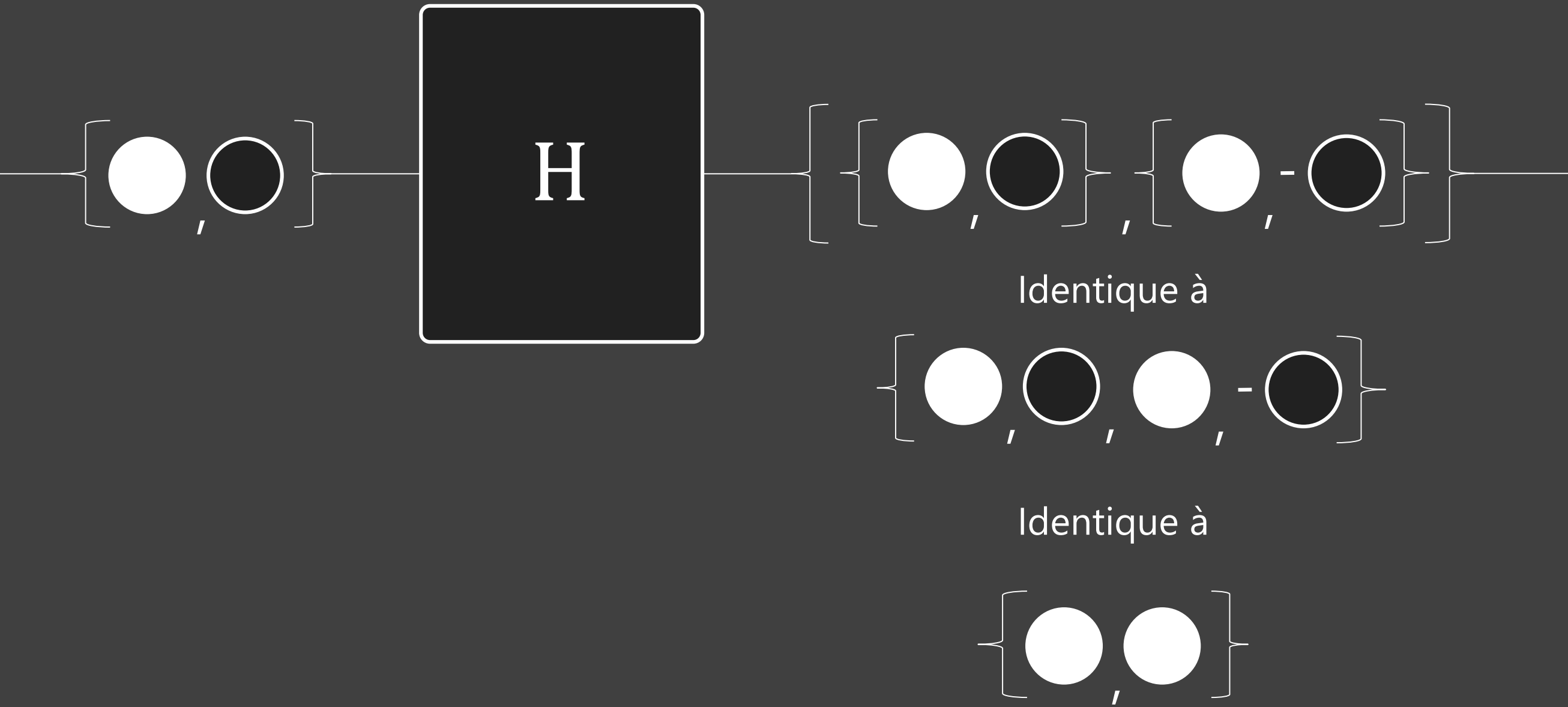


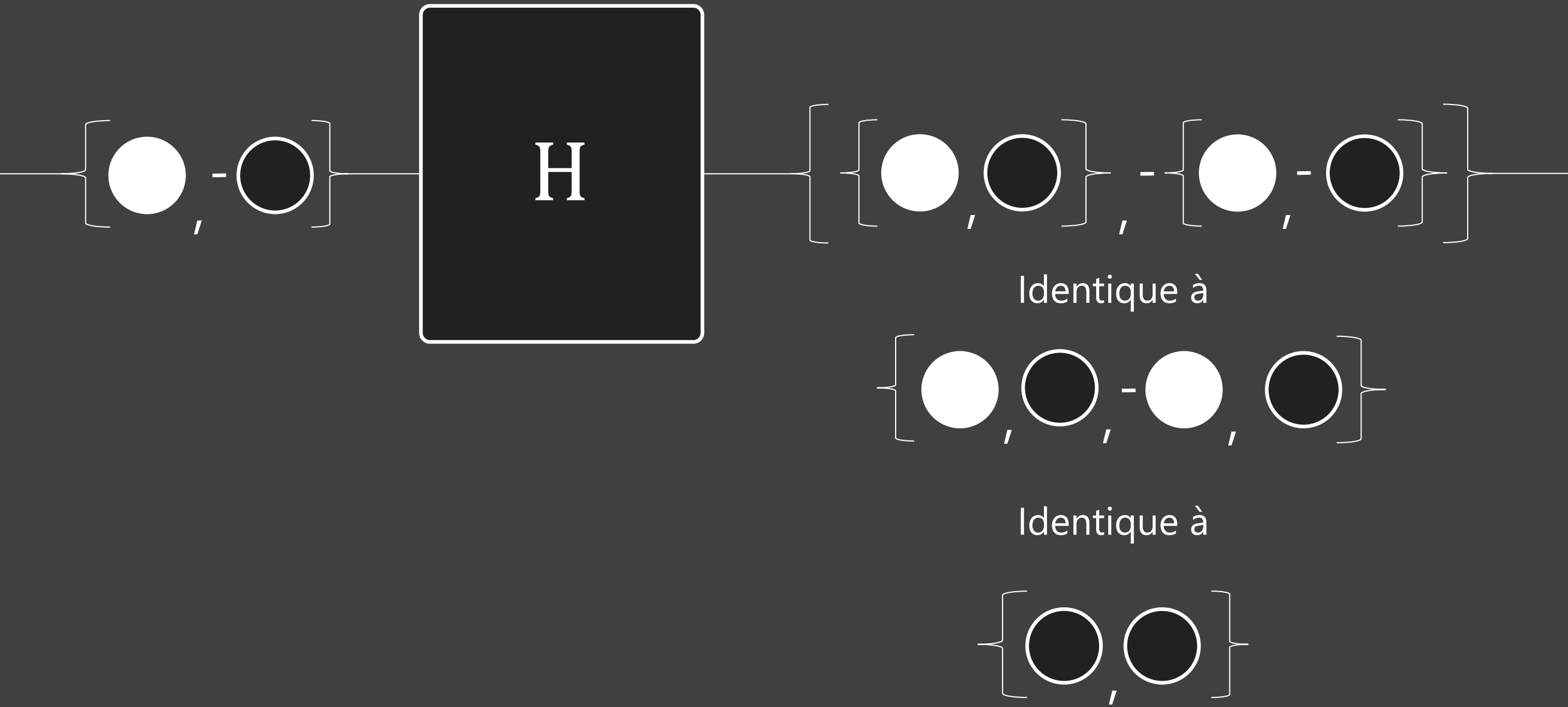












# QU'EST-CE QUE LA SUPERPOSITION ?

- L'état de superposition est une conséquence purement mathématique de la théorie quantique.
- L'interprétation physique pose problème, car cet état ne correspond à rien de connu en physique classique, et semble ne pas subsister à l'échelle macroscopique
- Il convient d'être très prudent quand on parle de particules « à plusieurs endroits en même temps » ou de chat « à la fois mort et vivant », car c'est appliquer des termes classiques, probablement inappropriés, à un état purement quantique

# QU'EST-CE QUE LA SUPERPOSITION ?

- Interprétations possibles de la superposition
  - Selon l'**interprétation de Copenhague** de la mécanique quantique, l'état quantique n'a pas de sens physique avant l'opération de mesure. Seul l'état projeté, après la mesure, a un sens physique. Ainsi, selon cette interprétation, il est vain de rechercher une signification physique à ce qui n'est et ne doit rester qu'une pure formule mathématique. Cette interprétation renie donc formellement toute formulation comme « plusieurs endroits en même temps », ou « mort et vivant ».
  - Selon la **théorie d'Everett**, défendue également par David Deutsch, l'état de superposition admet une interprétation physique. Les états superposés existeraient dans une infinité d'univers parallèles : la particule serait à une certaine position dans un univers, et à une autre dans un autre univers. Dans cette théorie il est impropre également de parler de « plusieurs endroits en même temps » : pas dans le même univers en tout cas.

# QU'EST-CE QUE LA SUPERPOSITION ?

- Selon l'interprétation de **De Broglie-Bohm**, la fonction d'onde n'est pas suffisante pour décrire totalement une particule, il faut lui adjoindre une position. Cette position est cependant inconnue de l'expérimentateur et n'est révélée que lors d'une mesure. Des particules préparées de la même façon ont alors la même fonction d'onde mais des positions différentes. Ainsi, selon cette interprétation, la position d'une particule est à chaque instant bien déterminée et ne peut en aucun cas être à « plusieurs endroits en même temps ». Cependant cette position est pilotée par la fonction d'onde qui est, quant à elle, définie en plusieurs endroits de l'espace simultanément.
- Aucune interprétation ne fait aujourd'hui l'unanimité des physiciens : à ce jour (2018), il s'agit d'un problème encore ouvert.

# QU'EST-CE QUE L'INTRICATION ?

- En mécanique quantique, l'intrication quantique, ou enchevêtrement quantique, est un phénomène dans lequel deux particules (ou groupes de particules) ont des états quantiques dépendant l'un de l'autre quelle que soit la distance qui les sépare
  - Observée lors d'une expérience célèbre par le physicien français Alain Aspect à l'Institut d'optique à Orsay entre 1980 et 1982
  - Des expériences démontrant ce phénomène ont été réalisées sur des distances de plus en plus grandes depuis les années 1970. En 2013, l'intrication a été prouvée sur deux électrons séparés de 1 300 mètres, et en 2017 des scientifiques chinois ont envoyé des photons enchevêtrés depuis un satellite à des stations terrestres séparées de 1 400 kilomètres

# QU'EST-CE QUE L'INTRICATION ?

- Paradoxe EPR (Einstein, Podolsky et Rosen) : expérience de pensée publiée dans un article de 1935 qui tentait de montrer que la mécanique quantique était incomplète. Notion d'« action fantôme à distance » [Einstein]
  - On démontre que les états intriqués ne peuvent pas être utilisés pour communiquer d'un point à un autre de l'espace-temps plus vite que la lumière. En effet, les états de ces deux particules sont seulement coordonnés et ne permettent pas de transmettre une information : le résultat de la mesure relatif à la première particule est toujours aléatoire.
  - Ceci est valable dans le cas des états intriqués comme dans le cas des états non-intriqués.
  - La modification de l'état de l'autre particule, pour instantanée qu'elle soit, conduit à un résultat tout aussi aléatoire.
  - Les corrélations entre les deux mesures ne pourront être détectées qu'une fois les résultats comparés, ce qui implique nécessairement un échange d'information classique, respectueux de la relativité...
  - La mécanique quantique respecte ainsi le principe de causalité.

# COMPARAISON BITS ET QUBITS

Classique	Quantique
1 bit a toujours une valeur définie	Pas de valeur définie tant qu'on ne l'observe pas
1 bit vaut seulement 0 ou 1	1 qubit peut être dans une superposition de 0 et de 1 simultanément
1 bit peut être copié sans être affecté	1 qubit dans un état inconnu ne peut pas être copié
1 bit peut être lu sans affecter sa valeur	Lire 1 qubit qui est initialement dans une superposition changera sa valeur
Lire 1 bit n'affecte pas un autre	Si 1 qubit est enchevêtré avec un autre qubit, en lire 1 affectera le second



Quelques applications

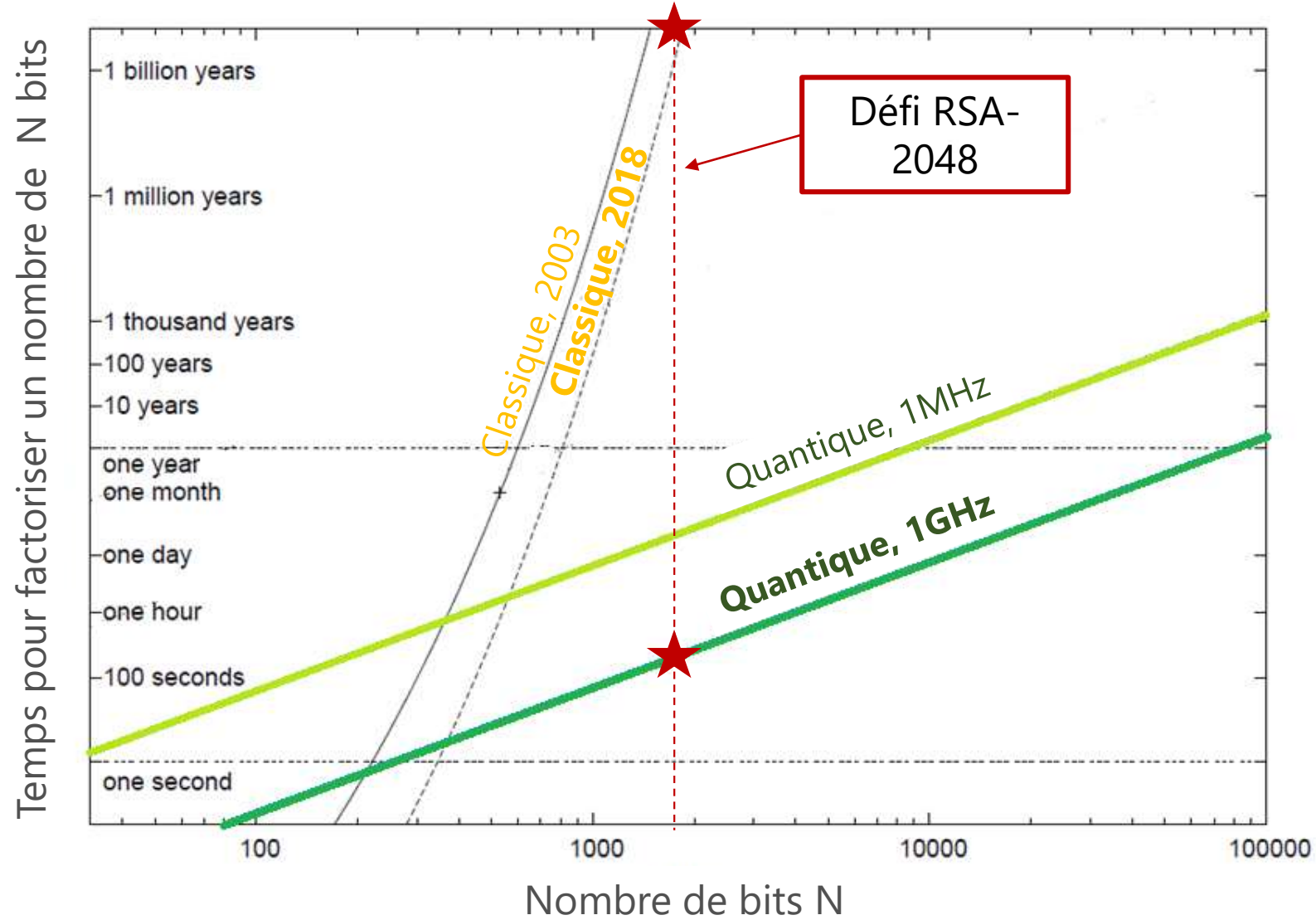
# Les problèmes classiquement insolubles

Classique

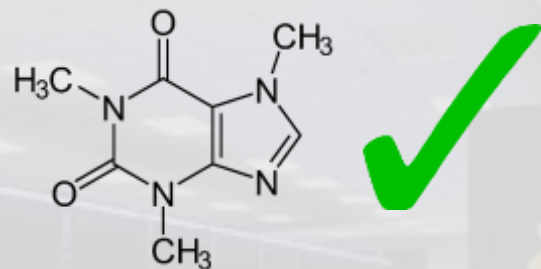
1 milliard  
d'années

Quantique

100 secondes



Casser l'algorithme RSA  
 (500 ordinateurs classiques)

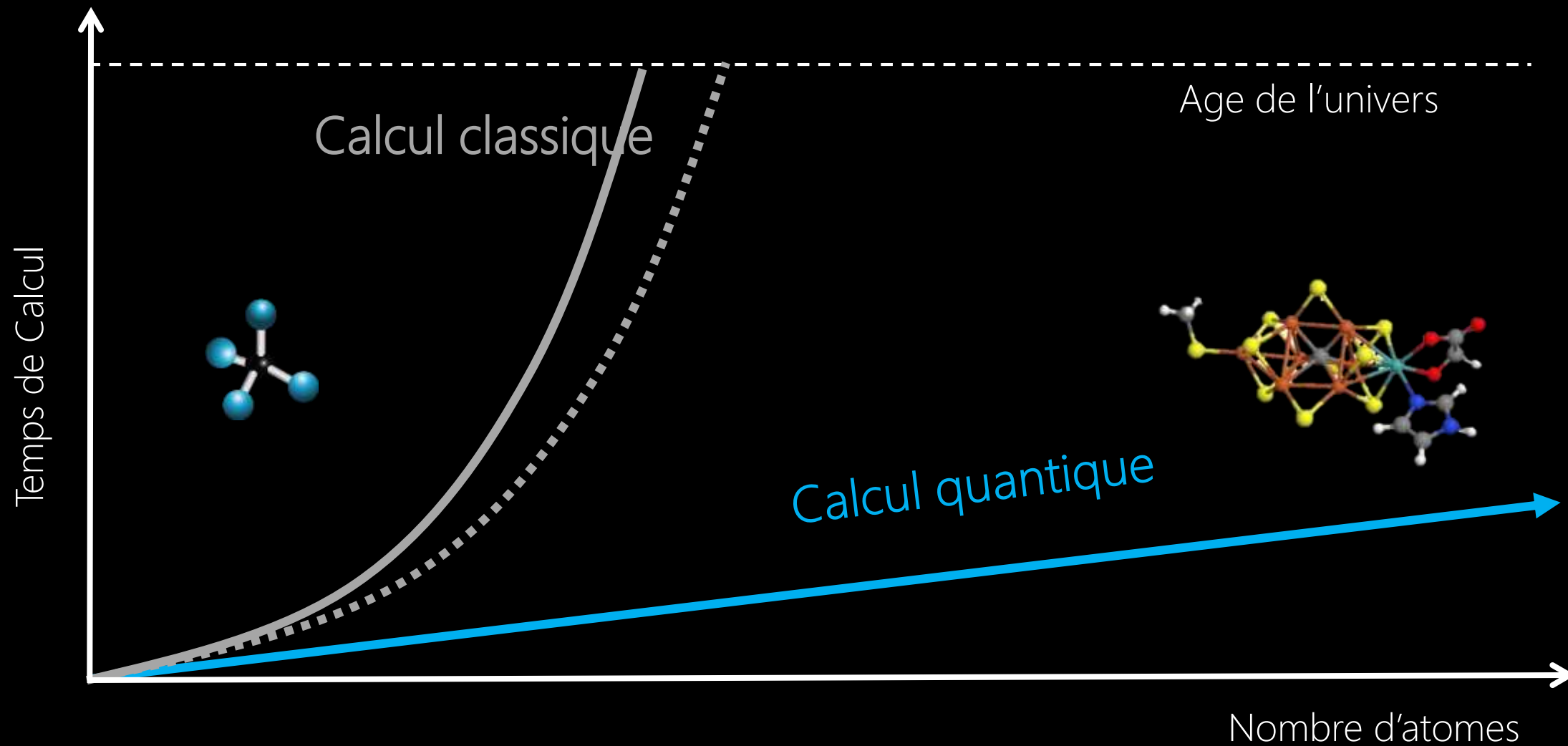


MOLECULE DE CAFEINE



COMPLEXE FEMOCO

Le supercalculateur le plus rapide du monde




○  
Adresser des problèmes classiquement insolubles

A photograph of a lush green cornfield in the foreground, with a sunset sky in shades of orange and blue in the background. A single white contrail is visible in the upper left portion of the sky.


Fixation de  
l'azote

A photograph of an industrial facility at sunset. A tall, dark smokestack is the central focus, emitting a thick plume of dark smoke that rises into the orange and blue sky. The silhouette of the factory building is visible at the bottom.

Capture du  
carbone

A photograph showing a perspective view of blue solar panels in the foreground. In the background, several high-voltage electrical transmission towers (pylons) are silhouetted against a blue sky with light clouds.

Science des  
matériaux

A photograph of a person's hand, wearing a light-colored sleeve, resting on the lid of a silver laptop. The laptop is open, and the background is a plain, light-colored surface.

Machine  
Learning

# Fixation de l'Azote

## Le problème :

Trouver un catalyseur pour convertir l'azote en ammoniac à température ambiante  
Réduire l'énergie pour convertir l'air en engrais

## Solution actuelle :

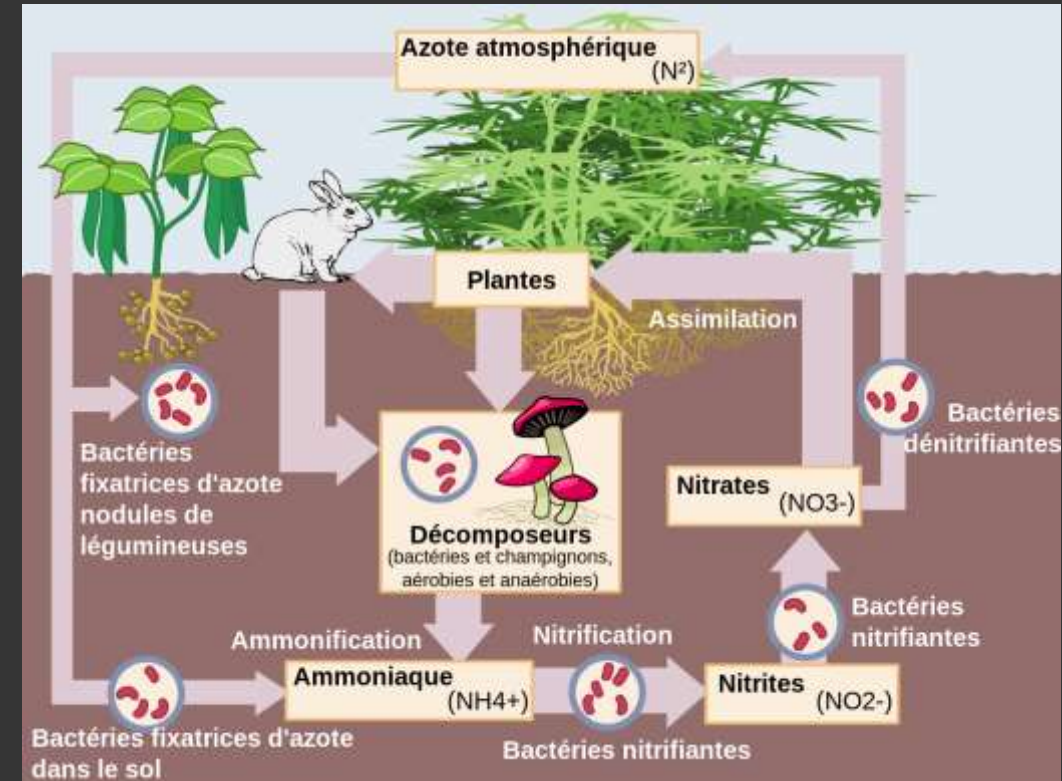
Utilisation du procédé de Haber inventé en 1909

Requiert hautes pressions et températures

Coût : 3-5% de la production de gaz naturel du monde entier (1-2% de l'énergie mondiale annuelle)

## Solution quantique :

~ 100-200 qubits : concevoir le catalyseur pour permettre une production non coûteuse d'engrais



# Capture du CO<sub>2</sub>

## Problème :

Trouver un catalyseur pour extraire le dioxyde de carbone de l'atmosphère

Réduire de 80-90 % la quantité de dioxyde de carbone

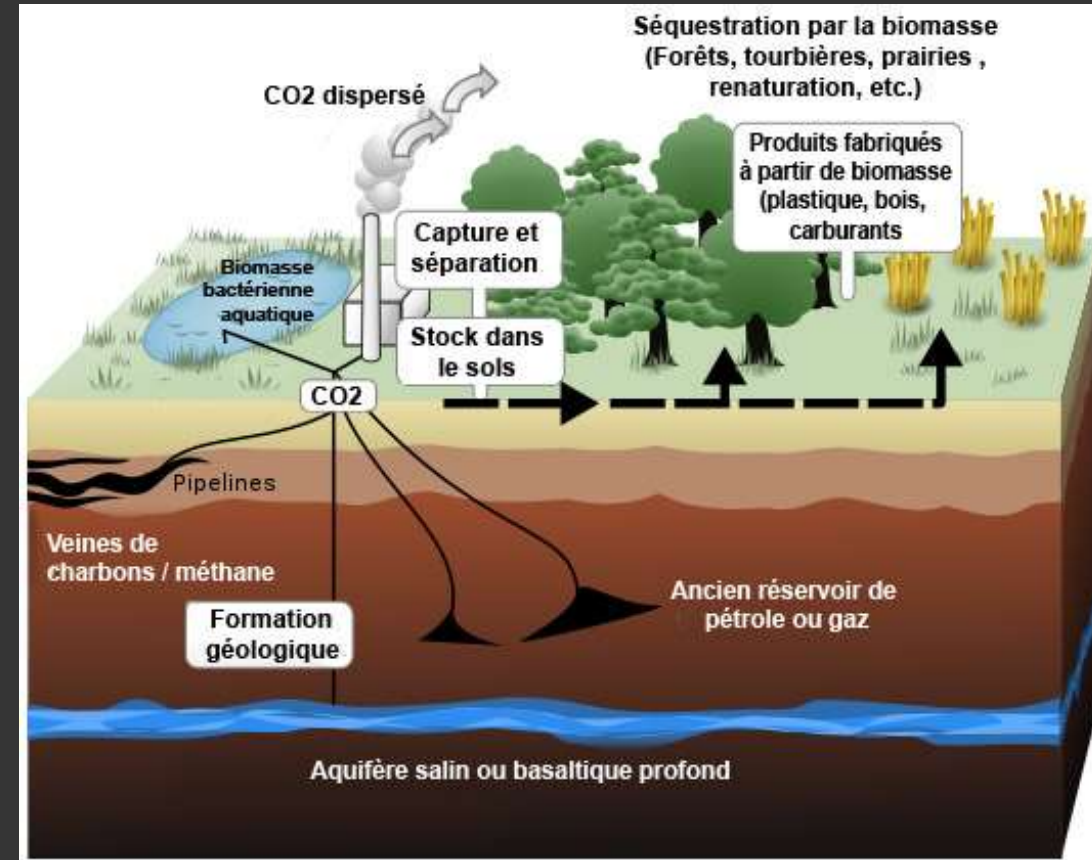
## Solution actuelle :

Capture sur des sources ponctuelles

Augmentation de 21-90% du coût énergétique

## Solution quantique :

~ 100-200 qubits : Concevoir un catalyseur pour permettre l'extraction du dioxyde de carbone de l'air



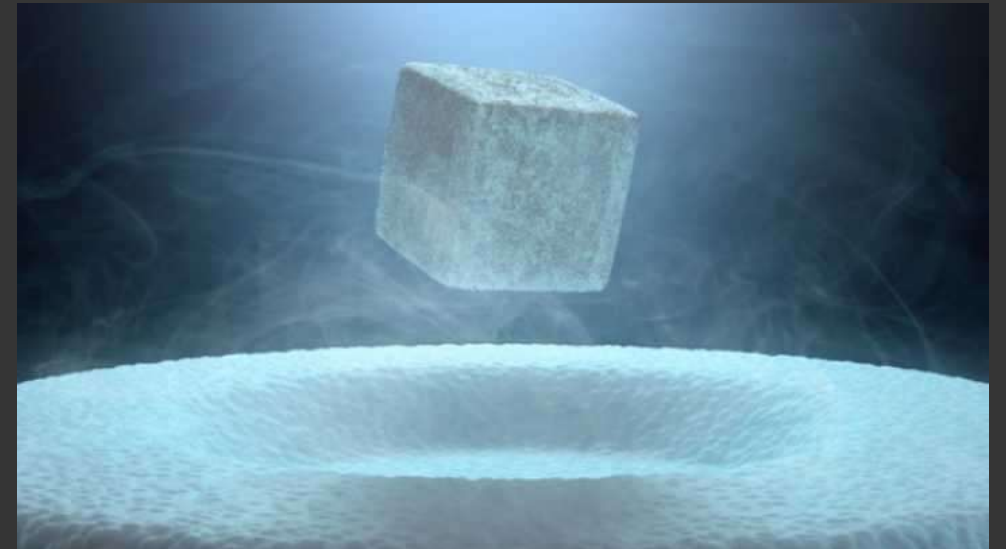


# Création d'un supraconducteur à température ambiante

## Problème :

Nous aimerions trouver un **matériau supraconducteur** à température ambiante. Qui affiche donc une résistance nulle à température ambiante.

Cela permettrait des inventions telles que des réseaux intelligents haute performance, la transmission de courant sans perte et les trains à sustentation magnétique.



## Solution quantique :

~ 100-200 qubits : résoudre l'équation de Schrödinger

# Machine Learning

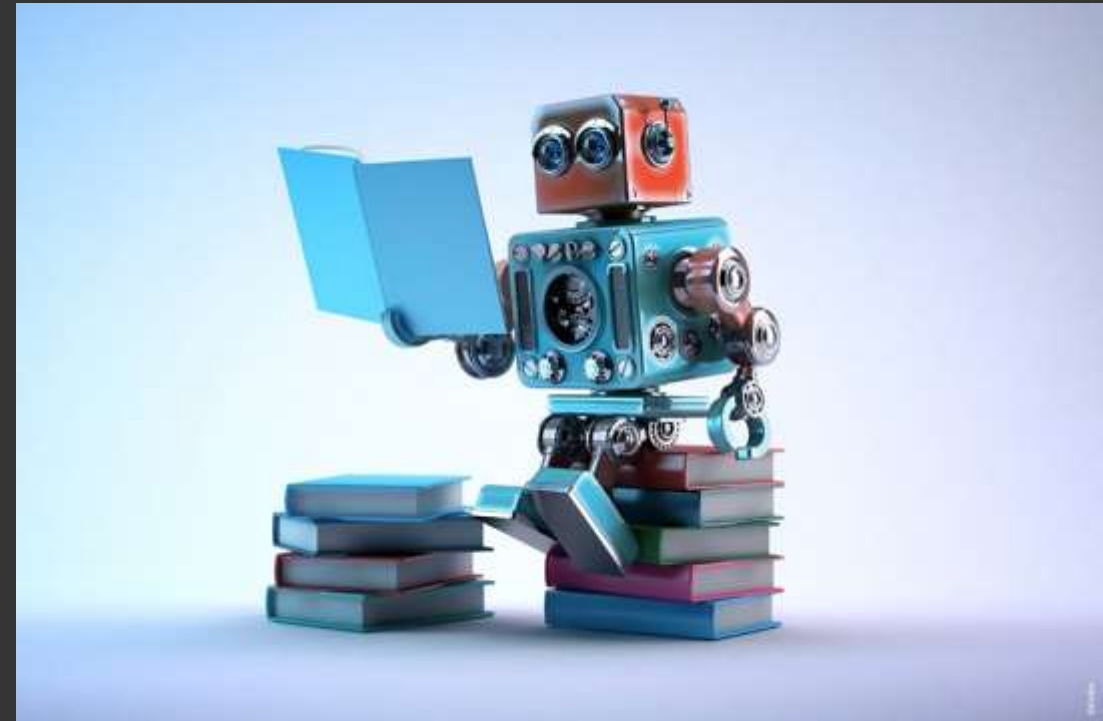
## Problème :

Les techniques actuelles du ML sont limitées à des approximations.

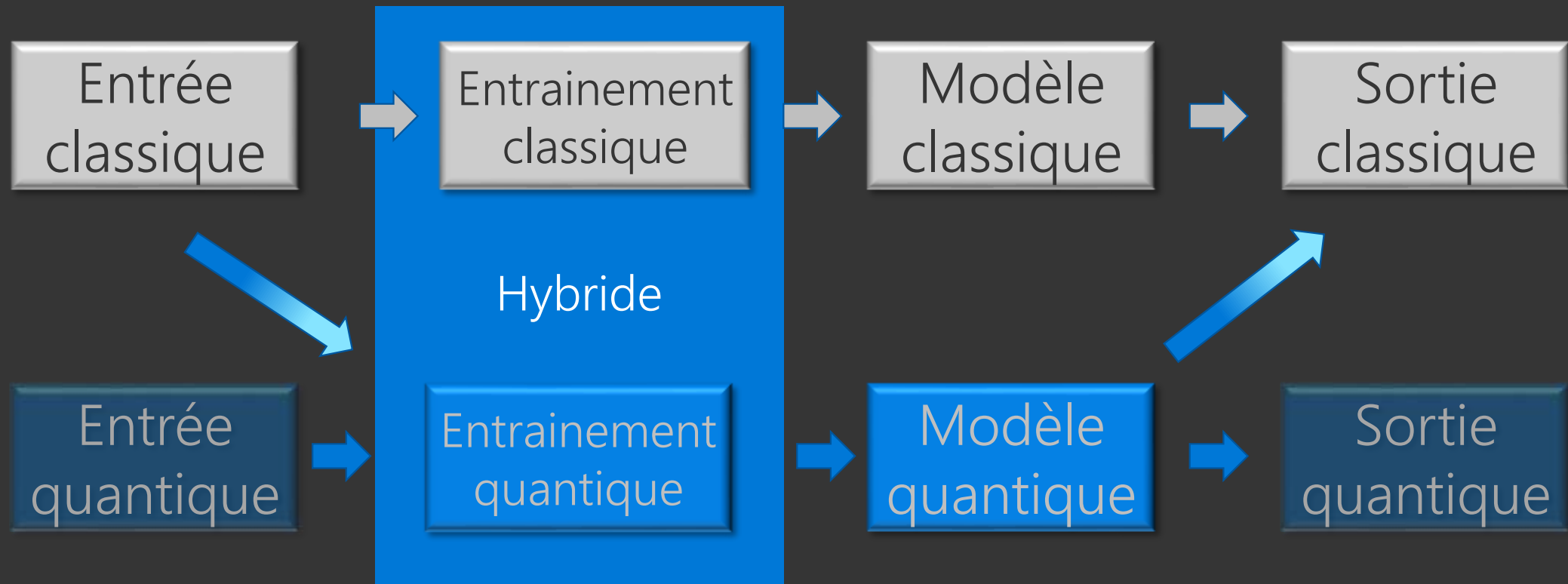
Par exemple, le Deep Learning, qui est très populaire pour la parole et la vision emploie des approximations car les solutions exactes sont inatteignables sur un ordinateur classique !

## Solution quantique :

~ 100-1000 qubits : deux voies : (1) Peut-on accélérer l'entraînement ? (2) Pouvons-nous apprendre un meilleur modèle ?

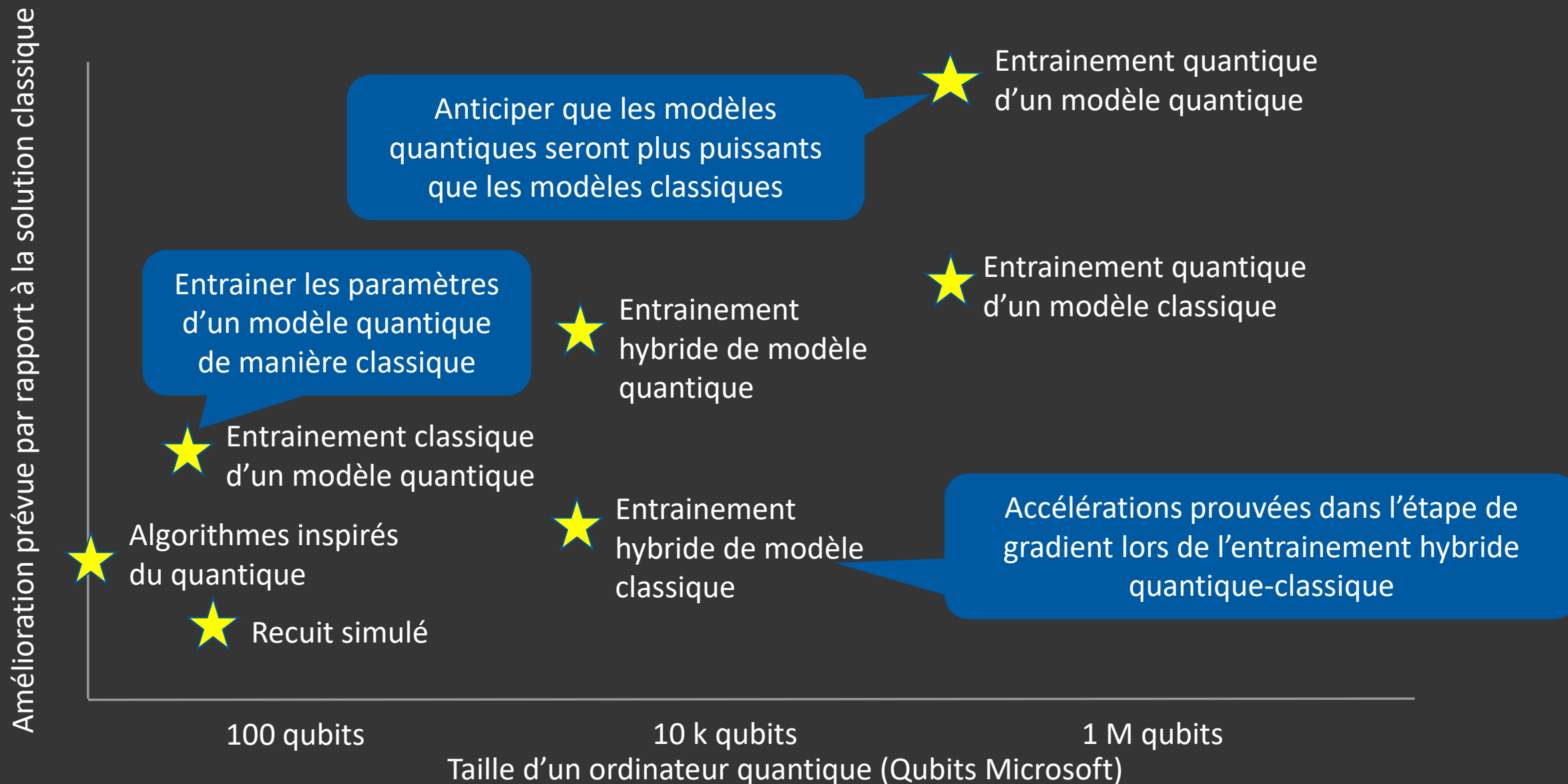


# Aujourd'hui : Entraîner un modèle classique avec une méthode classique



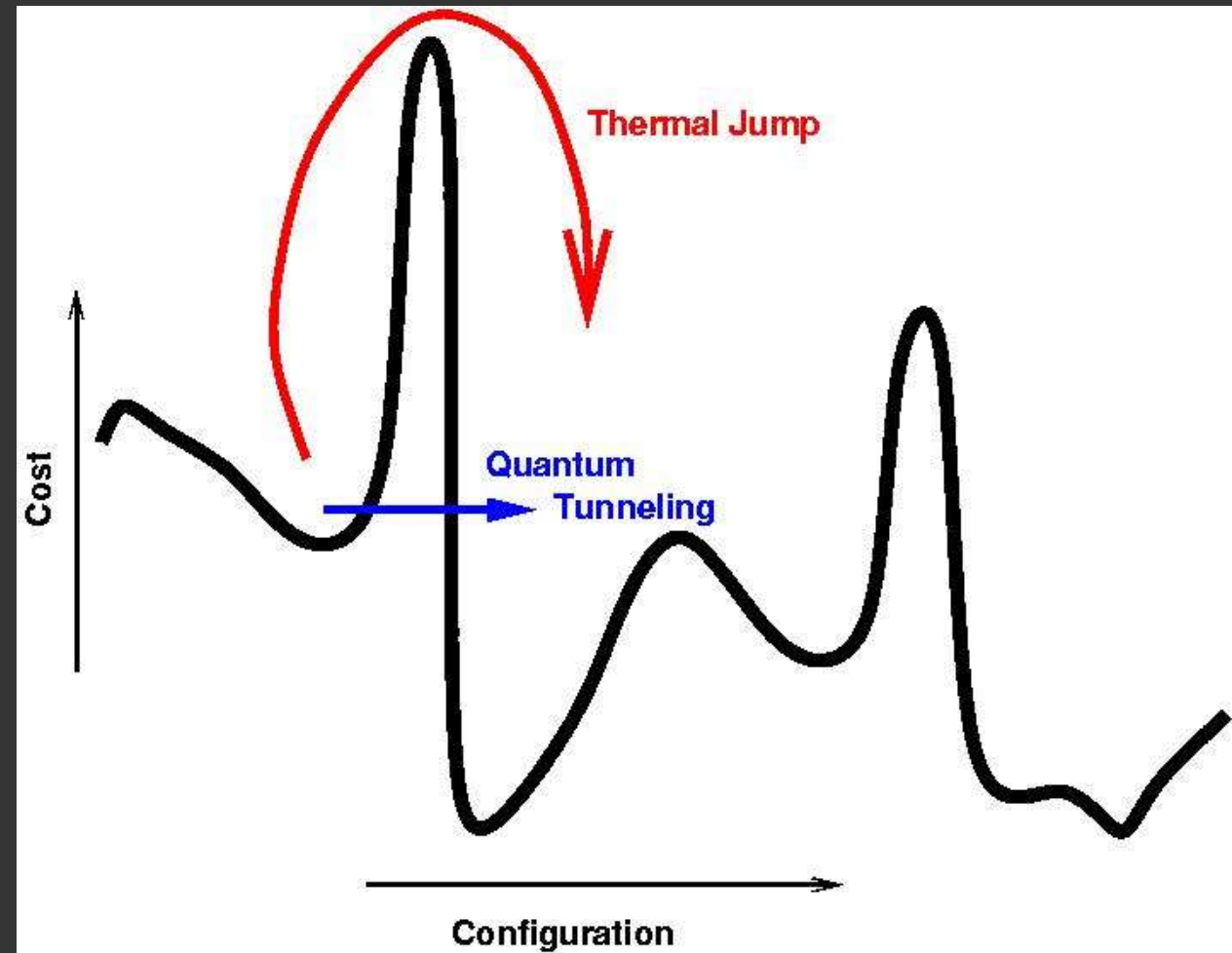
Demain : Utiliser une méthode améliorée par le quantique pour produire un meilleur modèle classique ou quantique

# Amélioration grâce au ML quantique

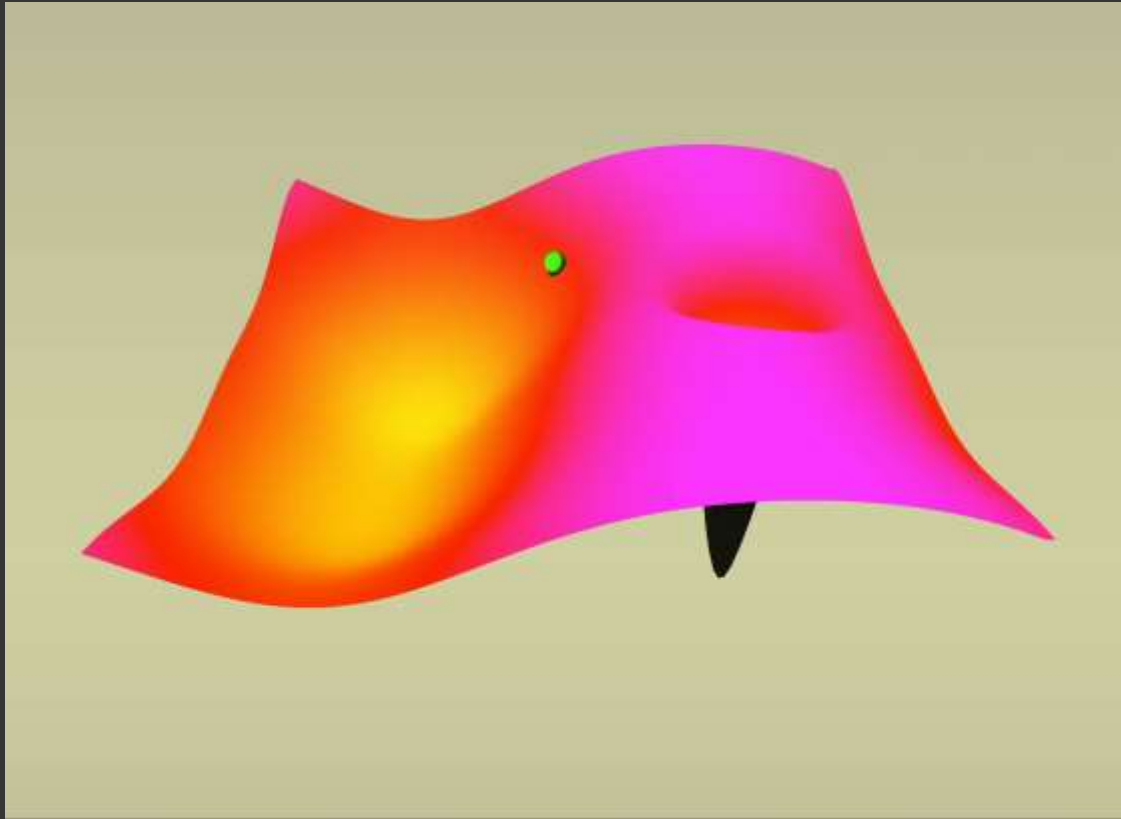


# Optimisation quantique

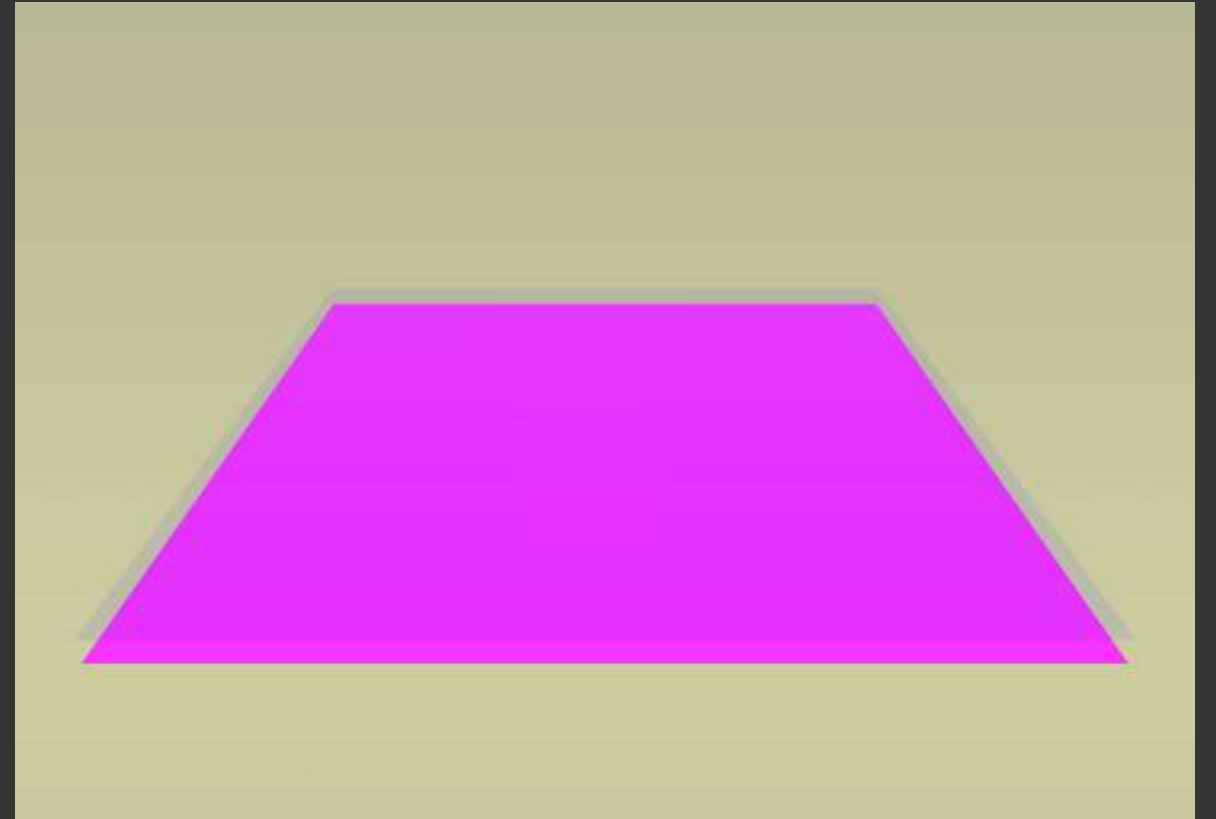
Utiliser des effets quantiques pour échapper à des minima locaux par effet tunnel sous une barrière



# Optimisation classique versus quantique



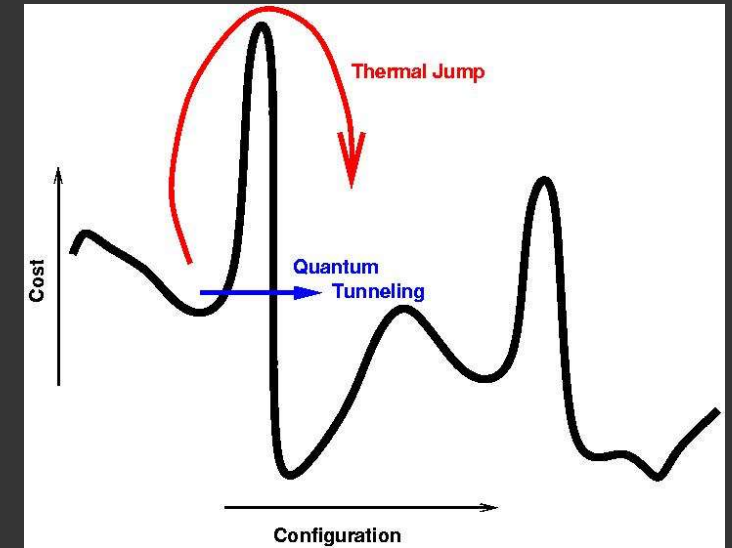
Classique



Quantique

# Première utilité : optimisation inspirée du quantique

Imiter l'effet tunnel quantique sur des ordinateurs classiques aujourd'hui !

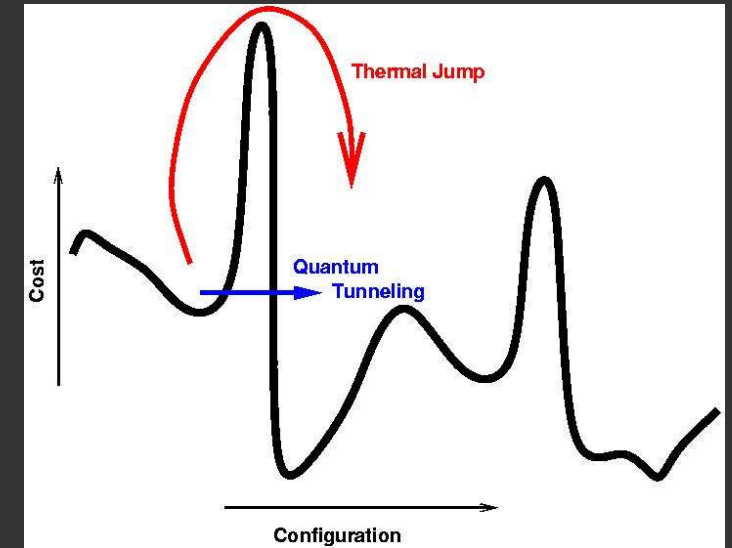


# Première utilité : optimisation inspirée du quantique

Imiter l'effet tunnel quantique sur des ordinateurs classiques aujourd'hui !

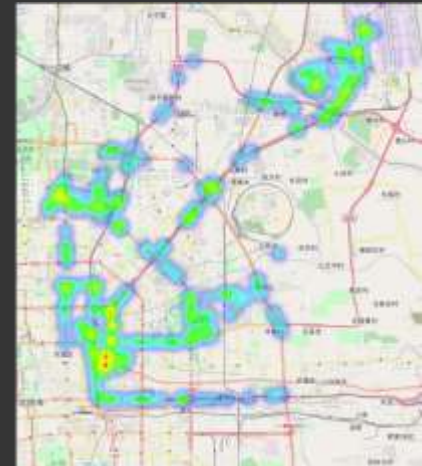
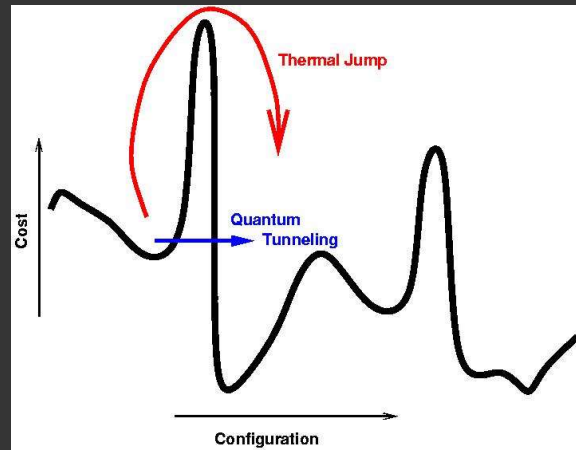
La recherche en **algorithmes quantiques** révèle souvent de nouveaux **algorithmes classiques**

Meilleures méthodes d'optimisation  
Meilleurs algorithmes d'entraînement  
Meilleurs modèles pour le Machine Learning





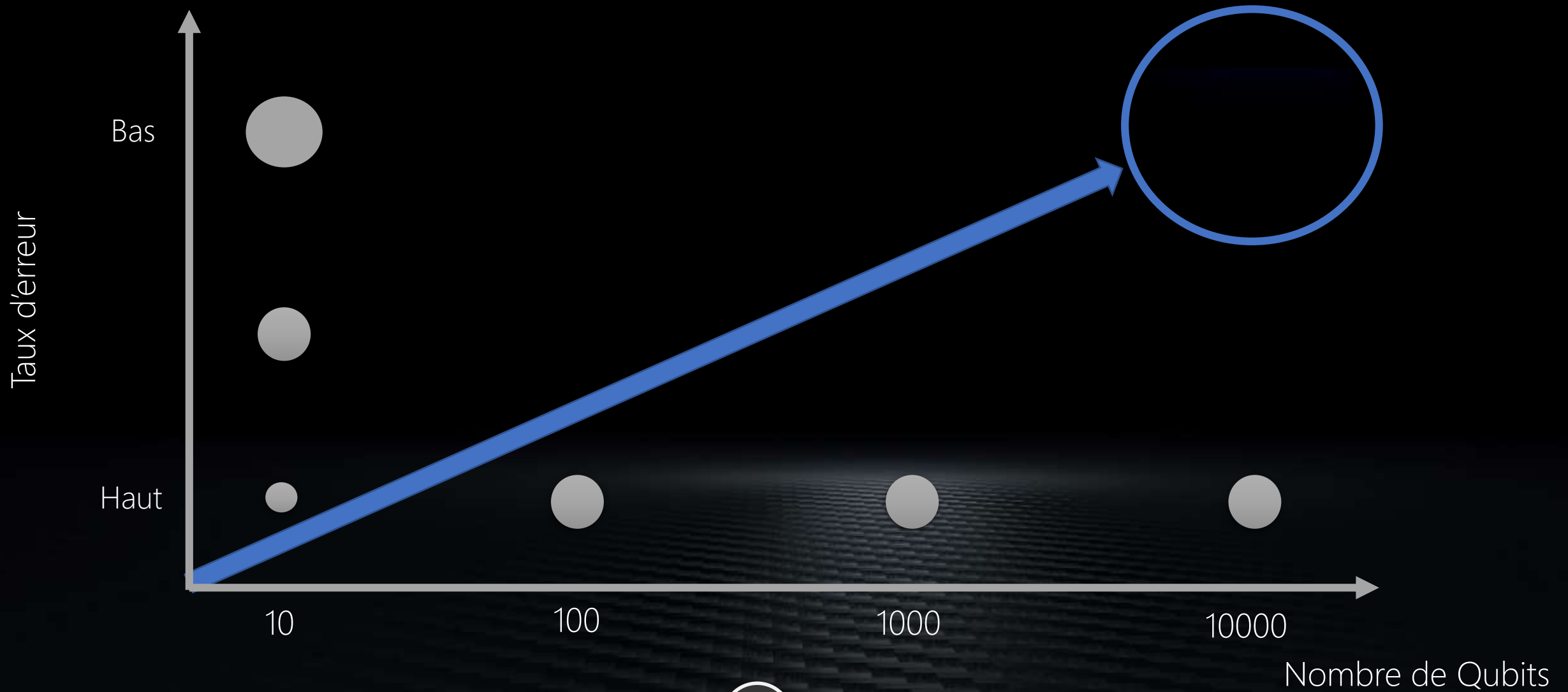
# Optimisation inspirée du quantique



Etude de cas : Un constructeur automobile a établi un partenariat avec D-wave pour résoudre des problèmes d'optimisation de trafic à Pékin :

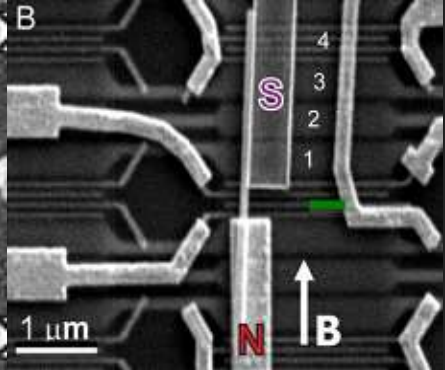
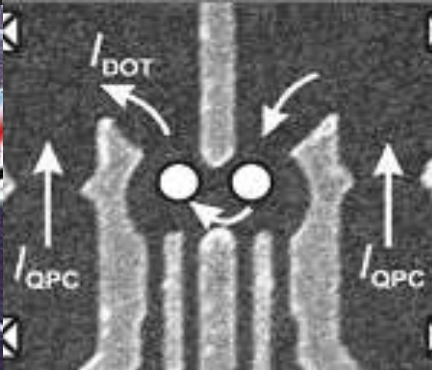
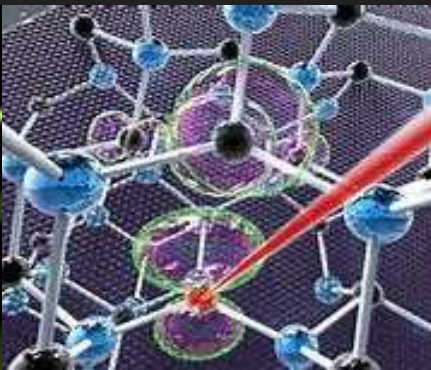
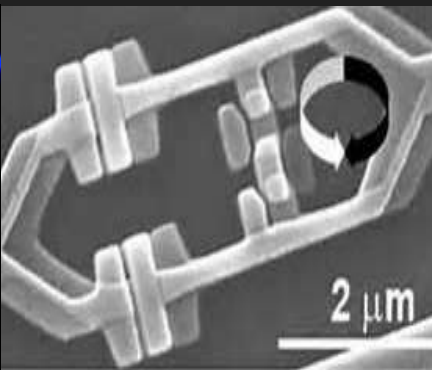
- Des heures pour le résoudre sur un supercalculateur
- 20 s pour le résoudre sur D-Wave (**40 fois plus vite**)
- Solution Microsoft inspirée du quantique : 200 ms pour le résoudre sur un PC ! (**4000 fois plus vite que sur un supercalculateur**)
- Encore plus rapide avec Brainwave (FPGA)

Concevoir un ordinateur quantique



Tous les qubits ne sont pas créés égaux

# TECHNOLOGIES HARDWARE QUANTIQUES



Pièges à Ion

Supra-  
conducteurs

Optique  
linéaire

Centres NV  
(azote-lacune)

Quantum  
dots

Topologique



Fermions de Majorana

Prédits par Ettore Majorana  
en 1937



# Inspiration

## Fault-tolerant quantum computation by anyons

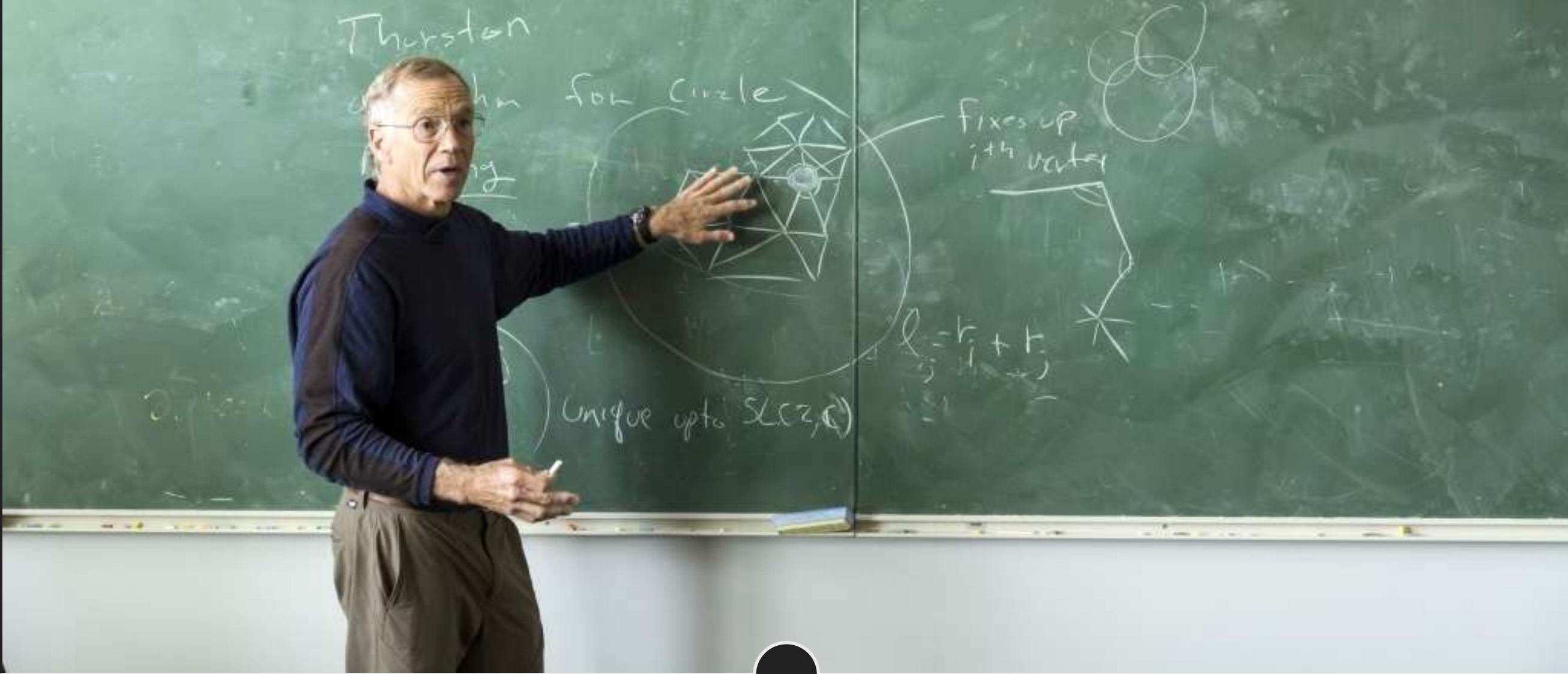
A. Yu. Kitaev

(Submitted on 9 Jul 1997)

A two-dimensional quantum system with anyonic excitations can be considered as a quantum computer. Unitary transformations can be performed by moving the excitations around each other. Measurements can be performed by joining excitations in pairs and observing the result of fusion. Such computation is fault-tolerant by its physical nature.

Comments: 27 pages, Latex2e, uses amssymb.sty, 13 Postscript figures  
Subjects: **Quantum Physics (quant-ph)**; Mesoscale and Nanoscale Physics (cond-mat.mes-hall); High Energy Physics - Theory (hep-th)  
Journal reference: Annals Phys. 303 (2003) 2-30  
DOI: [10.1016/S0003-4916\(02\)00018-0](https://doi.org/10.1016/S0003-4916(02)00018-0)  
Cite as: [arXiv:quant-ph/9707021](https://arxiv.org/abs/quant-ph/9707021)  
(or [arXiv:quant-ph/9707021v1](https://arxiv.org/abs/quant-ph/9707021v1) for this version)





2000

Les qubits topologiques offrent une fidélité 1000 à 10000 fois supérieure

# STATION

Q

The chalkboard contains several mathematical notes and a diagram:

- Left side:**  $\frac{P(h, m, p)}{1}$  and  $\sum_{abc}$
- Middle:**  $\delta \phi \delta_{m+n, 0} P_2(\dots)$
- Diagram:** A tree structure with nodes. The root node is labeled  $E$ . A vertical line descends from  $E$  through several nodes. To the right, a node is labeled  $L \rightarrow 10$  and  $L \rightarrow 10$ . Further right, a node is labeled  $j(z)$ . A circled node is labeled  $\textcircled{B}$ .
- Right side:**  $4 \langle f'(z) f(0) \rangle$  and  $\langle f'(z) f(0) \rangle$



2006





Science

25 May 2012 | \$16

AAAS

“

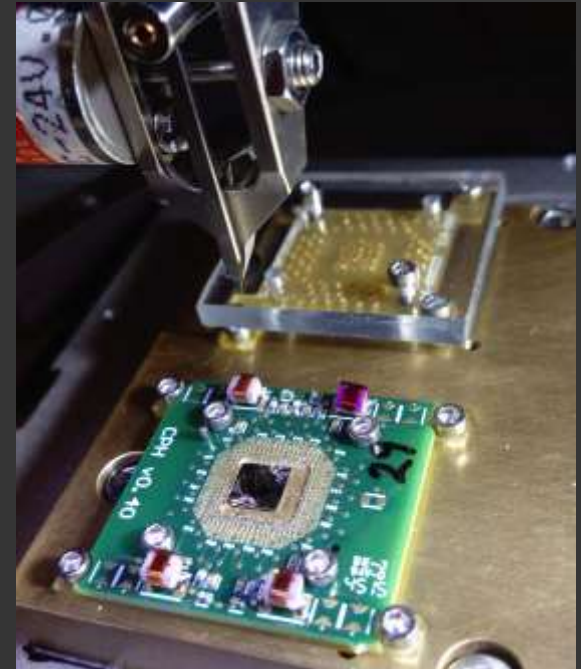
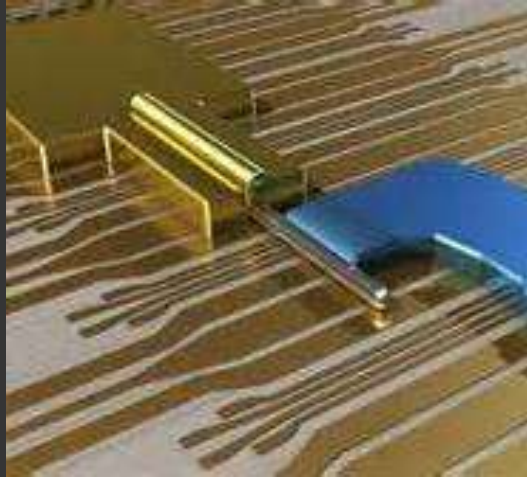
MAJORANA PARTICLE  
GLIMPSED IN LAB.

”

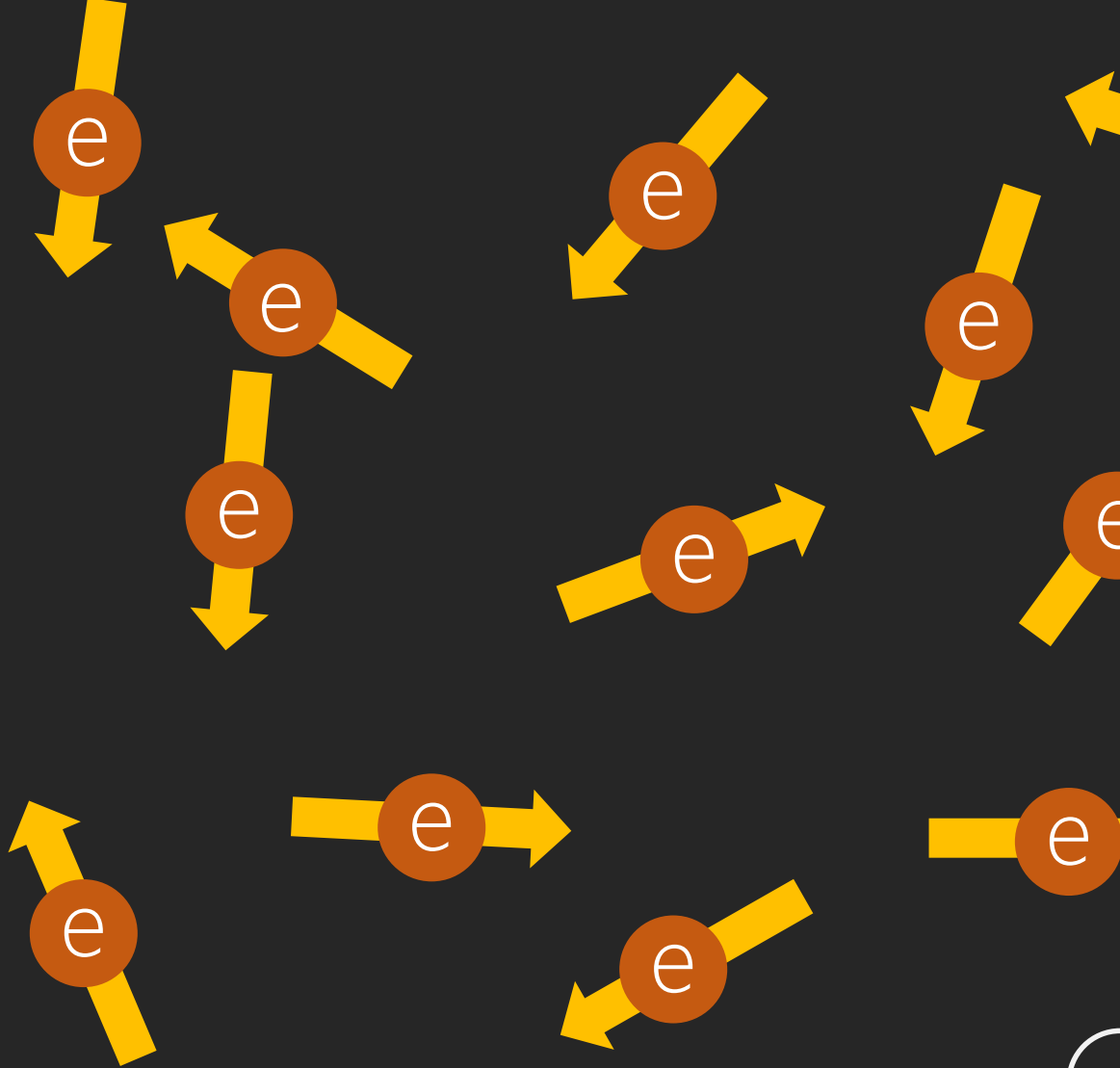
BBC NEWS

2012

# Développer et déployer un système quantique commercial évolutif pour résoudre les problèmes insolubles d'aujourd'hui



2018



Spin de l'électron



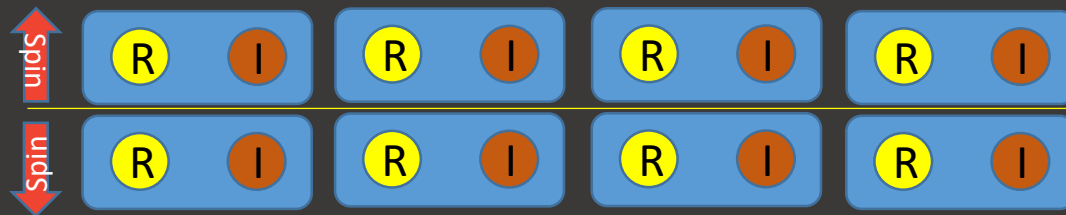


Fractionnalisation de l'électron

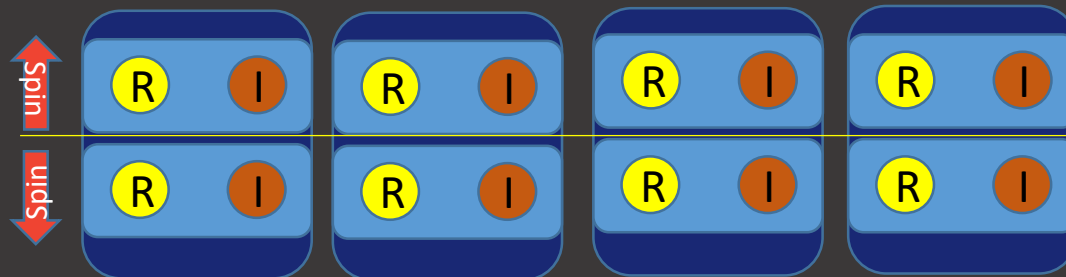


Superposition

Isolant :



Supraconducteur  
S-Wave Normal :

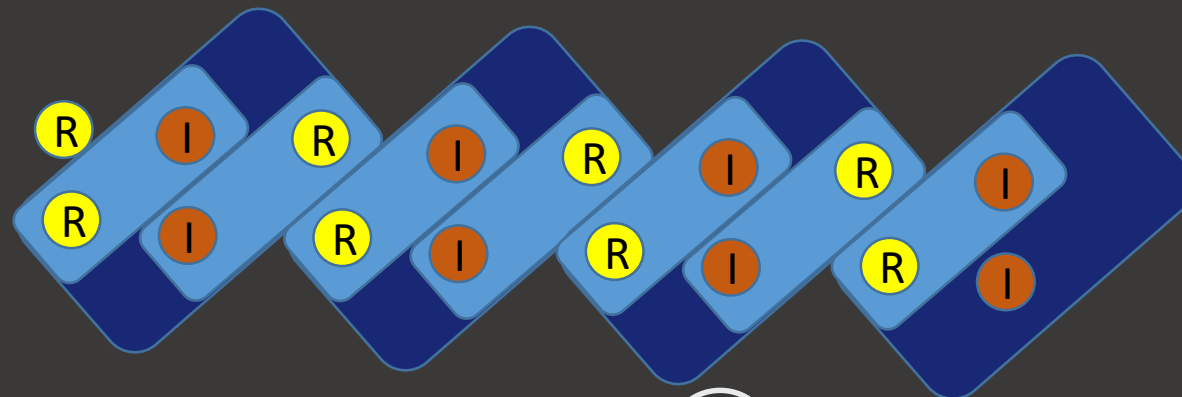


Paires de  
Cooper

Electron

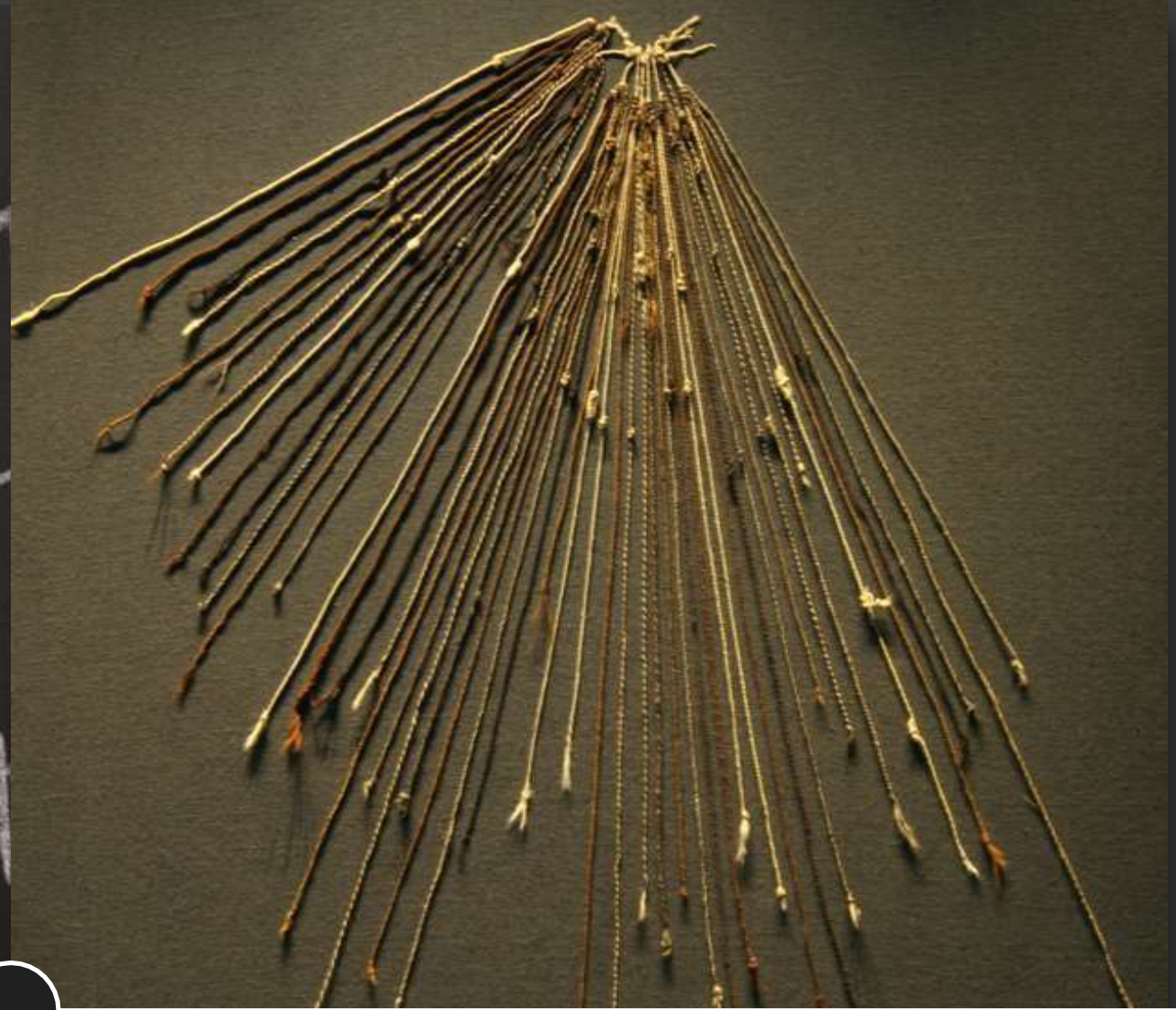
Paire

Supraconducteur  
S-Wave Normal :

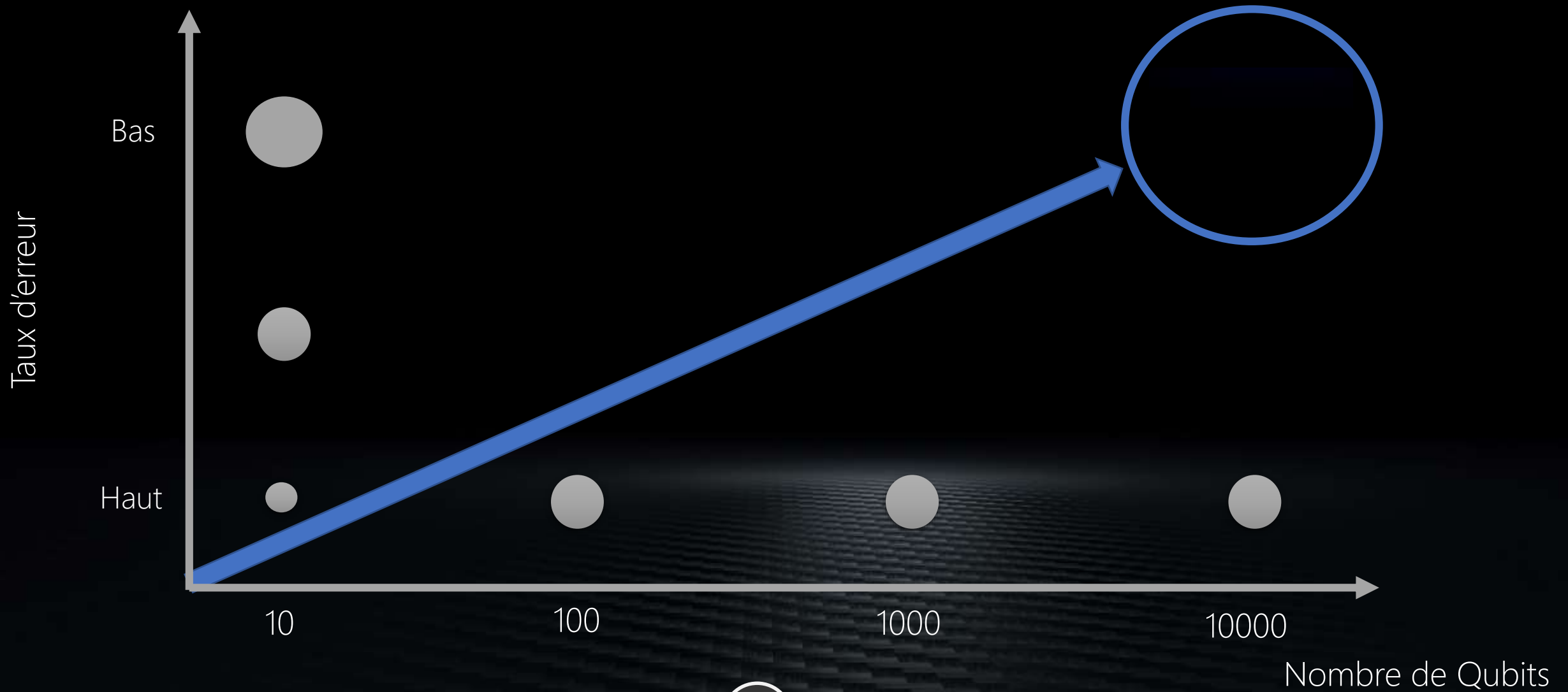


Fractionnalisation de l'électron

Superposition



Quipu Inca



Tous les qubits ne sont pas créés égaux

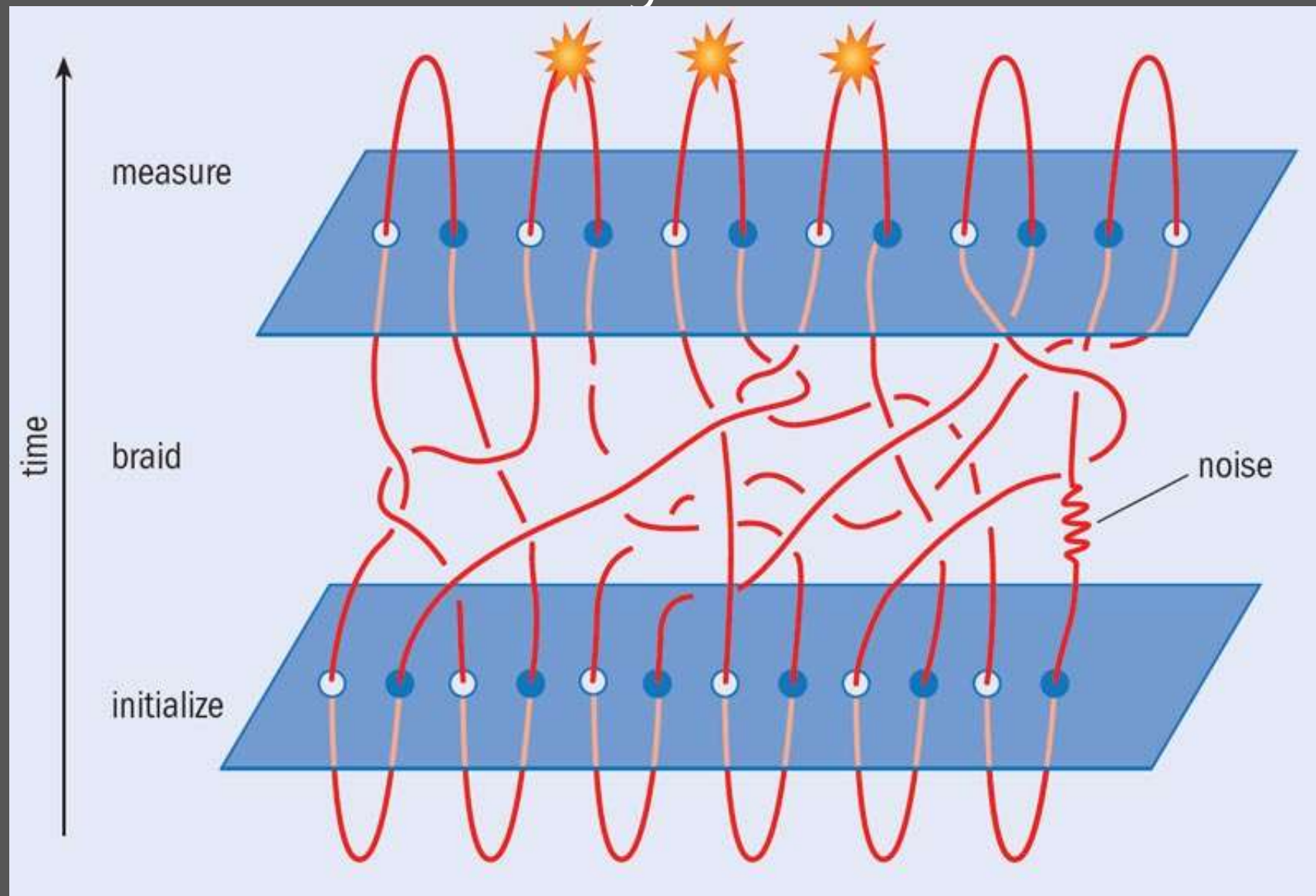


# Comparaison des technologies

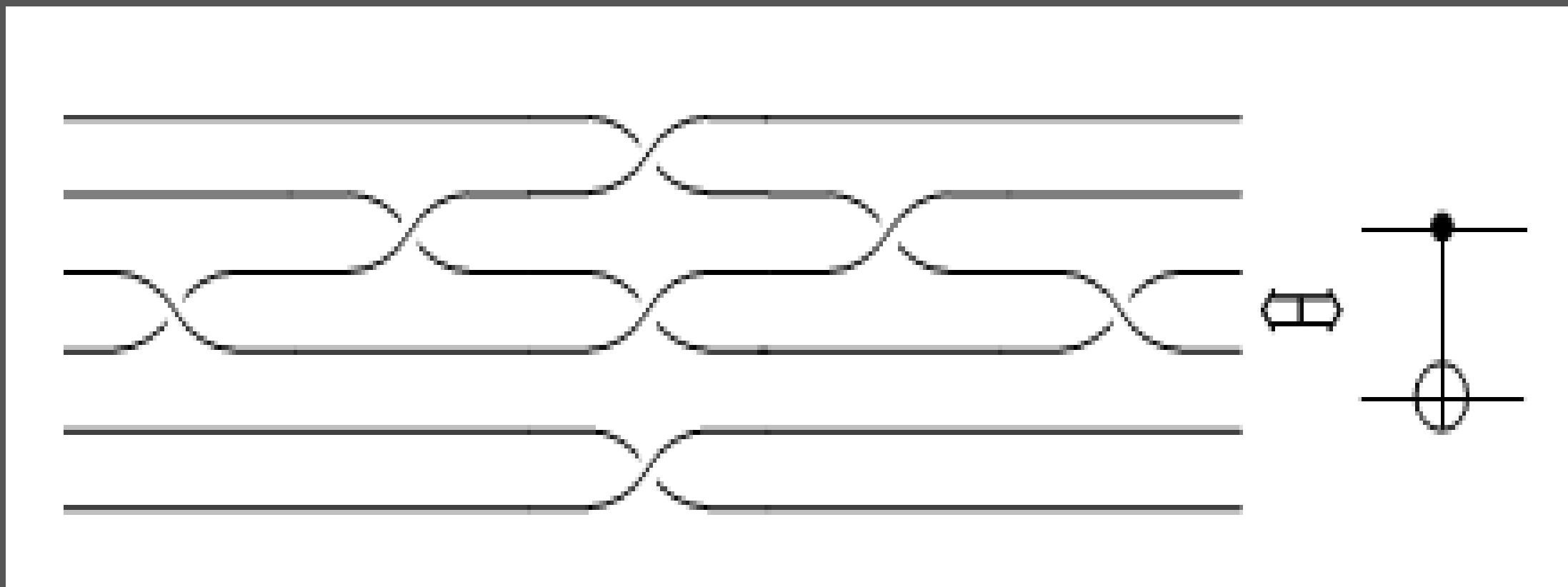
Technologies	Durée de vie	Vitesse de la porte	Coût de correction d'erreur
Topologique (Majorana)	1 minute	Nanosecondes	$10^1$
Flux Qubit	$/ 10^{10}$	Idem	$10^3 - 10^4$
Charge Qubit	$/ 10^{10}$	Idem	$10^3 - 10^4$
Transmon	$/ 10^7$	idem	$10^3 - 10^4$
Piège à Ion	$/ 10^2$	$10^3$ plus lent	$10^3 - 10^4$

- La correction d'erreur est extrêmement difficile (pas de « quantum refresh » comme avec une DRAM)
- La plupart peuvent être fabriquées grâce à des variations des techniques semiconducteur classiques

# Tresser les fermions de Majorana



L'exemple de la porte quantique CNOT  
Une porte CNOT est l'équivalent réversible  
quantique d'une porte XOR



# L'approche unique de Microsoft



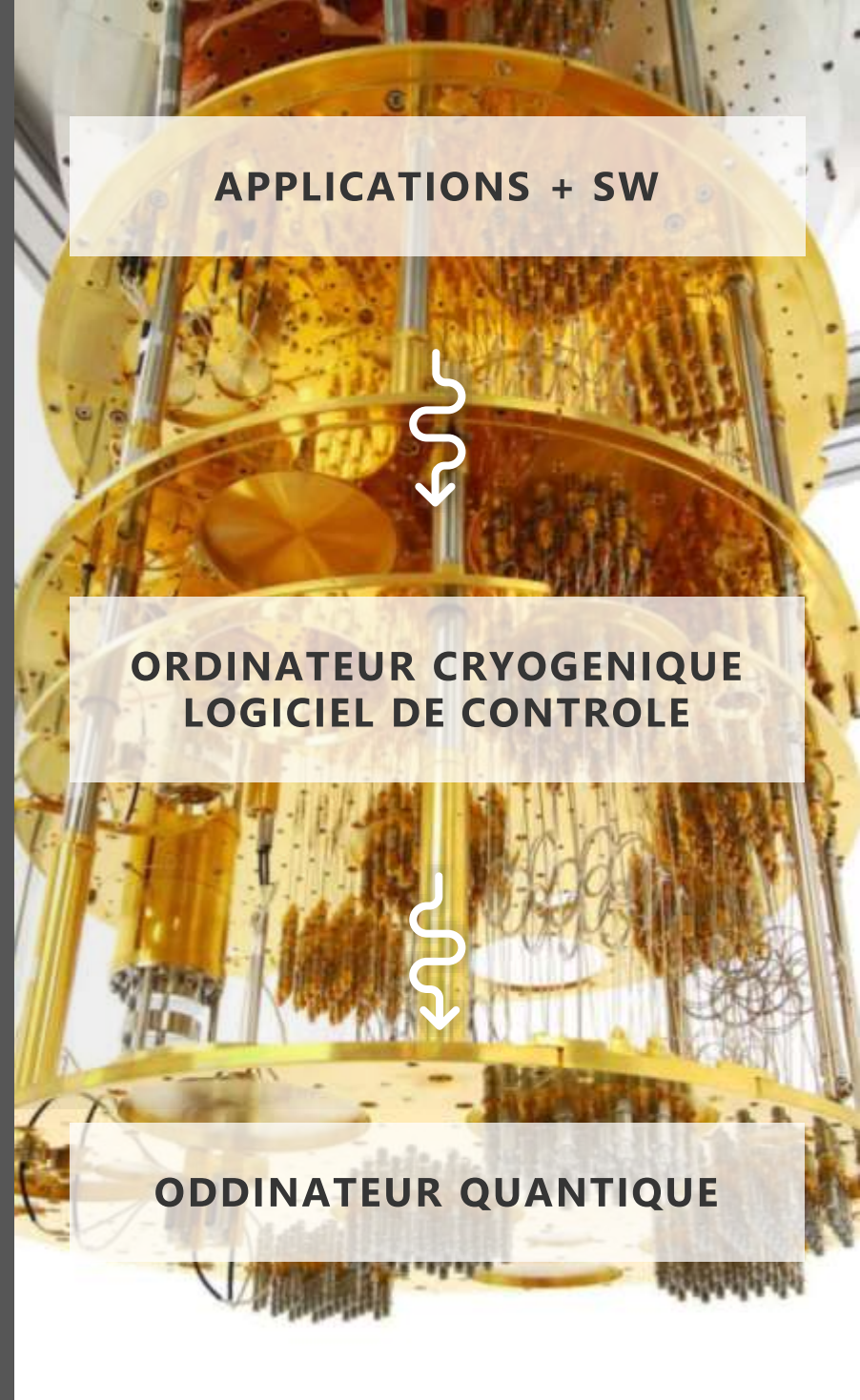
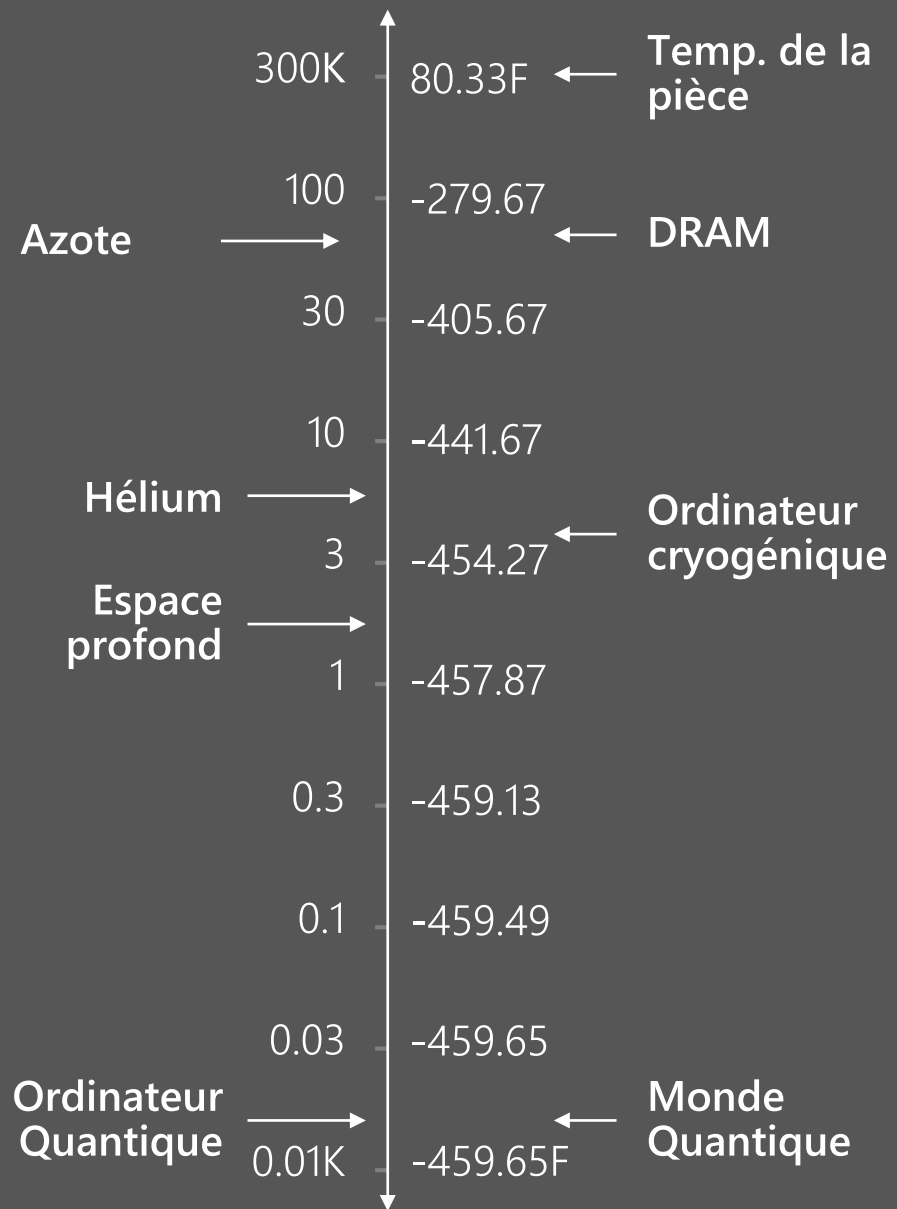
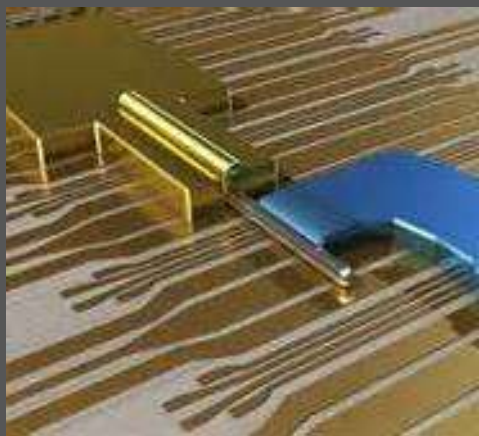
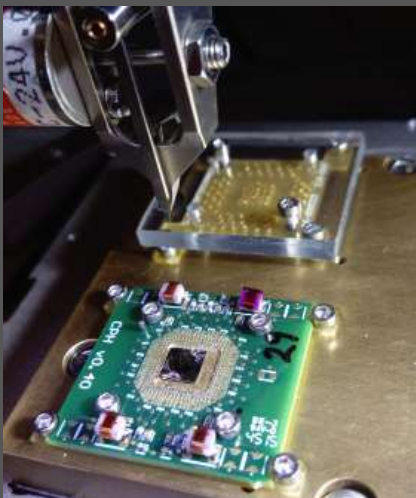
**Approche topologique  
révolutionnaire**



**Des investissements audacieux et  
une équipe mondiale**



**Technologie évolutive, de bout  
en bout**



**APPLICATIONS + SW**

**ORDINATEUR CRYOGENIQUE  
LOGICIEL DE CONTROLE**

**ORDINATEUR QUANTIQUE**

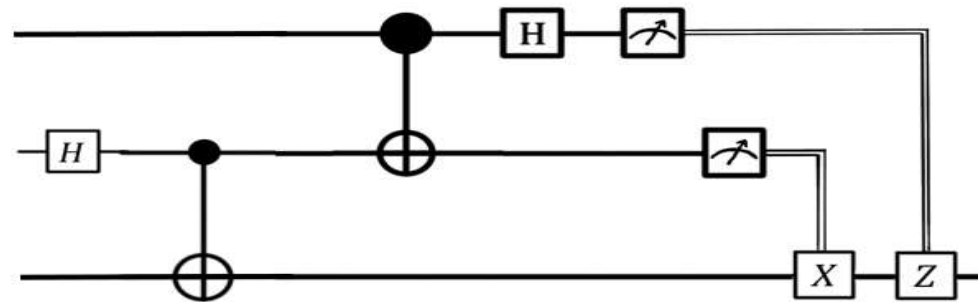
# Trois grands niveaux d'abstraction

L'approche  
de pile  
complète de  
Microsoft

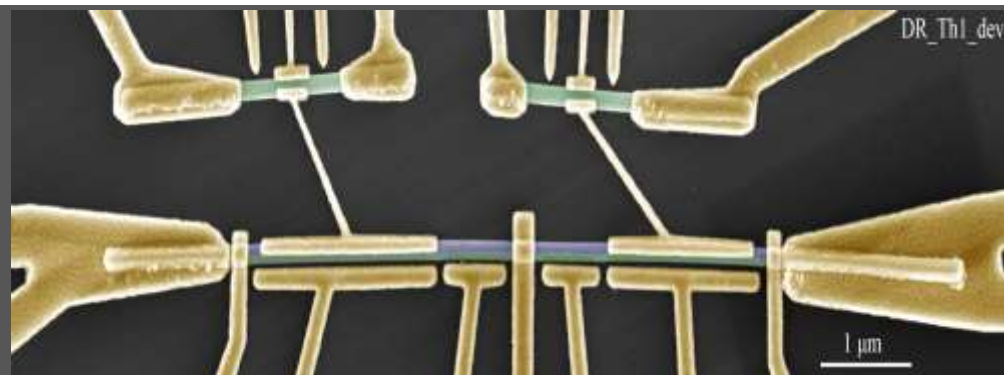
Algorithmes Quantiques

```
operation Teleport(alice : Qubit, bob : Qubit) : () {  
  body {  
    using (register = Qubit[1]) {  
      let temp = register[0];  
      H(temp);  
      CNOT(temp, bob);
```

Langage machine  
Quantique

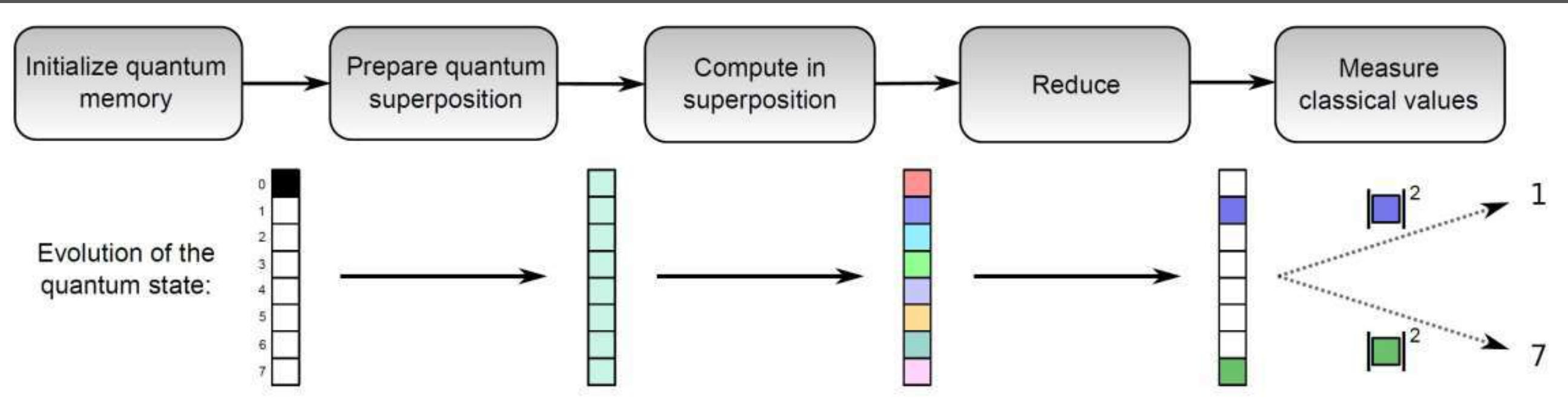


Hardware Quantique



# Calculer dans une situation de superposition

~~Les ordinateurs quantiques sont rapides car ils opèrent sur toutes les valeurs à la fois~~



Ce n'est pas facile !

- Lire depuis la superposition ne nous donne qu'une seule entrée aléatoire
- L'aspect crucial de la conception d'un algorithme quantique est de trouver les bonnes opérations de réduction qui conduisent à des réponses (presque) déterministes

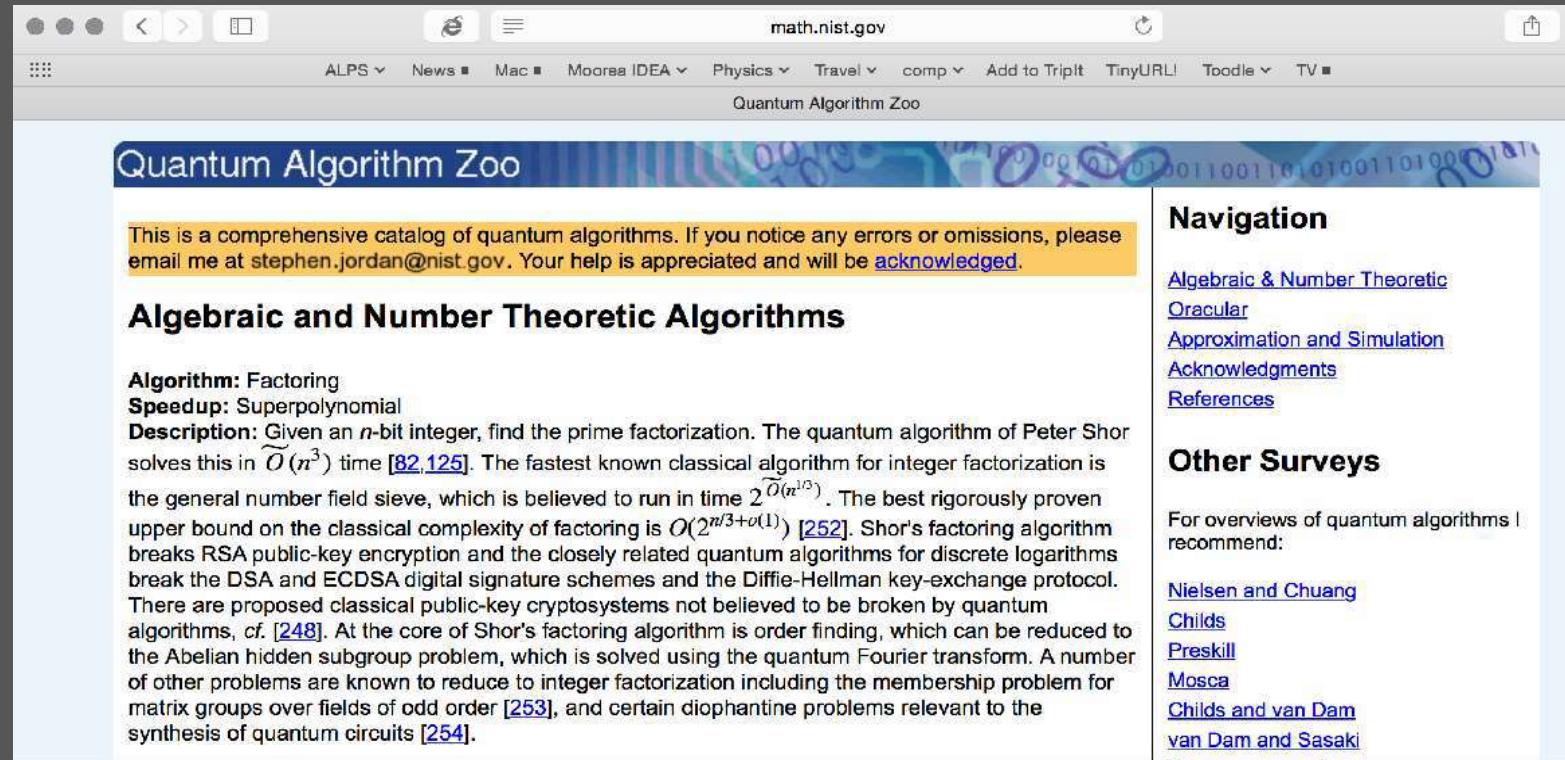
# Développer des applications quantiques

1. Trouver un algorithme quantique avec une accélération de performances quantique



# Algorithmes quantiques permettant une accélération quantique

- 50+ algorithmes quantiques permettant une accélération quantique qui est meilleure qu'un passage à l'échelle asymptotique sur n'importe quel ordinateur classique



The screenshot shows a web browser window with the URL [math.nist.gov](http://math.nist.gov). The page title is "Quantum Algorithm Zoo". A yellow banner at the top reads: "This is a comprehensive catalog of quantum algorithms. If you notice any errors or omissions, please email me at [stephen.jordan@nist.gov](mailto:stephen.jordan@nist.gov). Your help is appreciated and will be [acknowledged](#)." Below this, the section "Algebraic and Number Theoretic Algorithms" is displayed. The first entry is "Factoring", with a "Speedup: Superpolynomial" and a "Description" that details Peter Shor's algorithm, its complexity  $\tilde{O}(n^3)$ , and its application in breaking RSA, DSA, and ECDSA. A "Navigation" sidebar on the right lists categories like "Algebraic & Number Theoretic", "Oracular", "Approximation and Simulation", "Acknowledgments", and "References". Another sidebar titled "Other Surveys" lists authors like Nielsen and Chuang, Childs, Preskill, Mosca, Childs and van Dam, and van Dam and Sasaki.

<http://math.nist.gov/quantum/zoo/>

# Développer des applications quantiques

Ingénieurs logiciels quantiques

1. Trouver un algorithme quantique permettant une accélération de performances quantique
2. Confirmer l'accélération quantique après avoir implémenté toutes les sous-routines et les I/O
3. Optimiser le code jusqu'à ce que le temps d'exécution soit assez court
4. Intégrer dans une architecture spécifique et estimer les ressources

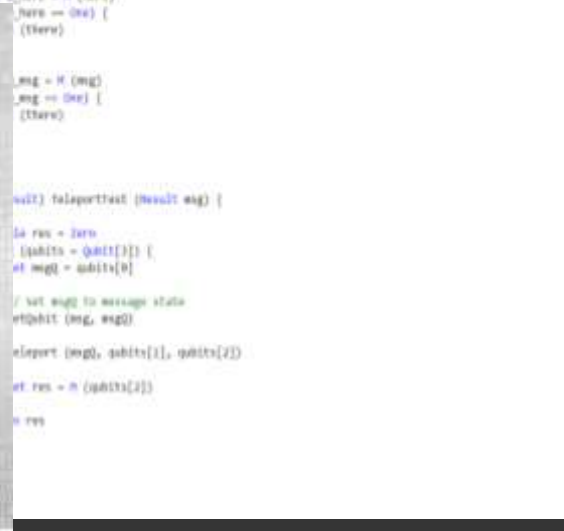
# Il est temps d'écrire du logiciel quantique

Explorer des applications quantiques

Inventer de nouveaux algorithmes quantiques

Optimiser du code quantique

```
Microsoft Visual Studio  
File Edit View Project Build Debug Team Test Architecture Test Analyze Window Help  
Solution Explorer  
TQuantique  
1 operation () EPR (qubit 02, qubit 03) {  
2   body {  
3     H (02)  
4     CNOT (02,03)  
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 a_here = H (there)  
15    here -- One) [ (there)  
16  
17    msg = H (msg)  
18    msg -- One) [ (there)  
19  
20    wait teleportFast (Result msg) {  
21  
22    let res = Zero  
23    (qubits = qubits[]) {  
24      let msg2 = qubits[0]  
25  
26      // set msg2 to message state  
27      wqubit (msg, msg2)  
28  
29      teleport (msg2, qubits[1], qubits[2])  
30  
31      let res = H (qubits[2])  
32  
33    } res
```

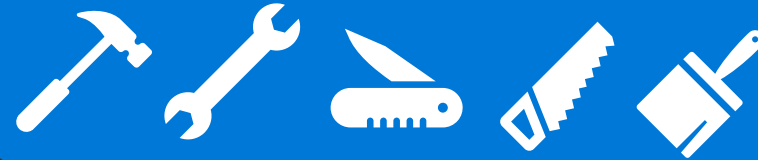


# De bons outils rendent possible le saut quantique !



« Plateforme » quantique

Kit de  
développement  
quantique



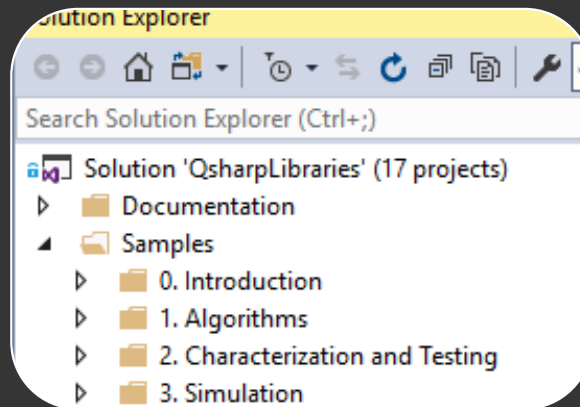
Outils quantiques

# Microsoft Quantum Development Kit

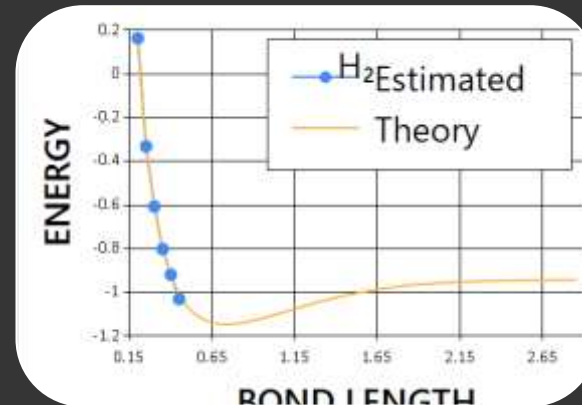
```
// ## there
/// A qubit initially in the |0> state that
/// the state of msg to.
operation Teleport(msg : Qubit, there : Qubit)
  body {
    using (register = Qubit[1]) {
      // Ask for an auxillary qubit that
      // for teleportation.
      let here = register[0];

      // Create some entanglement that
      H(here);
      CNOT(here, there);
    }
  }
}
```

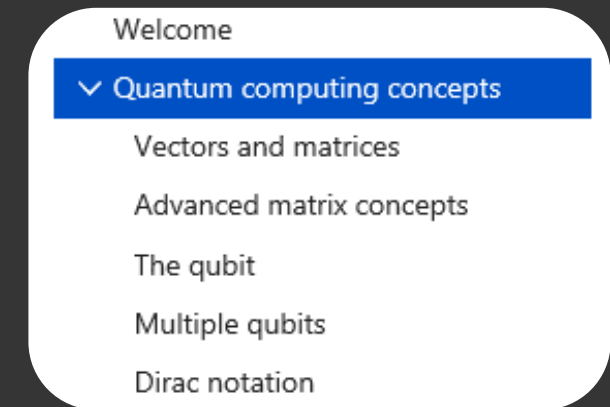
Langage de  
programmation  
quantique



Intégration Visual  
Studio  
et débogage



Simulation  
quantique locale  
et Cloud



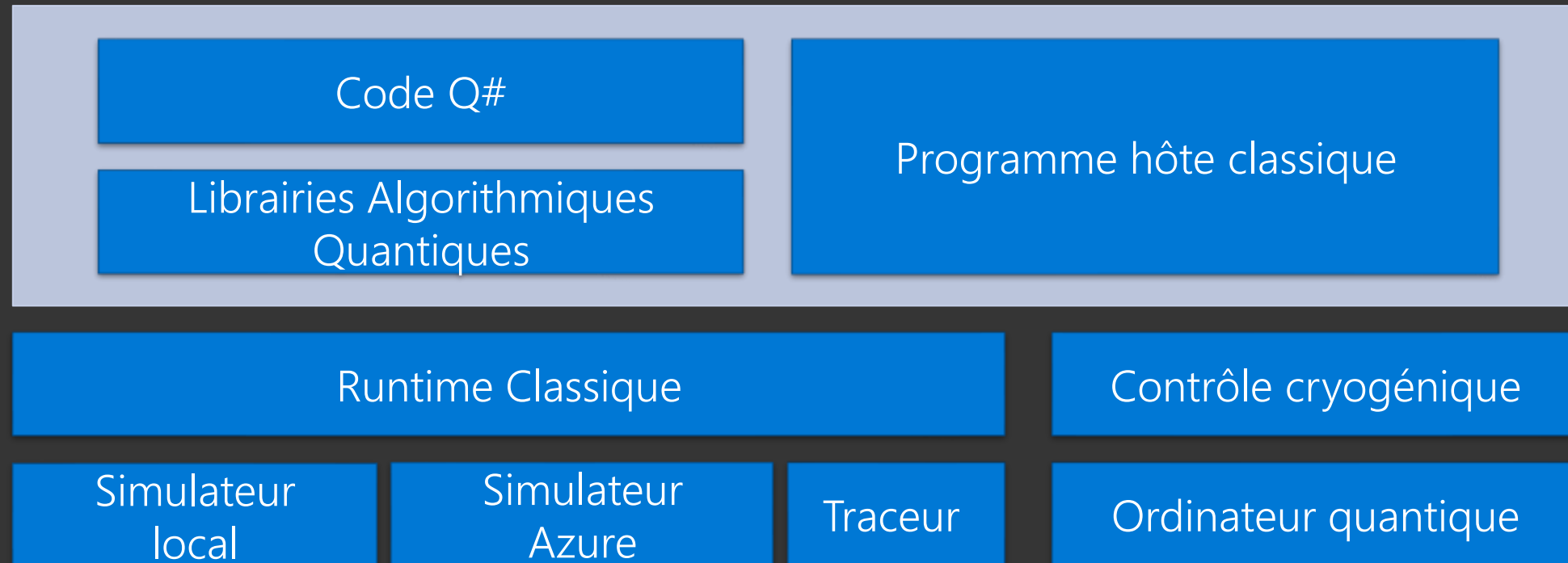
Librairies  
complètes,  
exemples et  
documentation

# Langage de programmation quantique : Q#

- *Domain-specific language* pour algorithmes quantiques et développement
- De type fonctionnel
- Intégration Visual Studio
- Fonctionnalités spécifiques au quantique
- Bibliothèques complètes, exemples et documentation

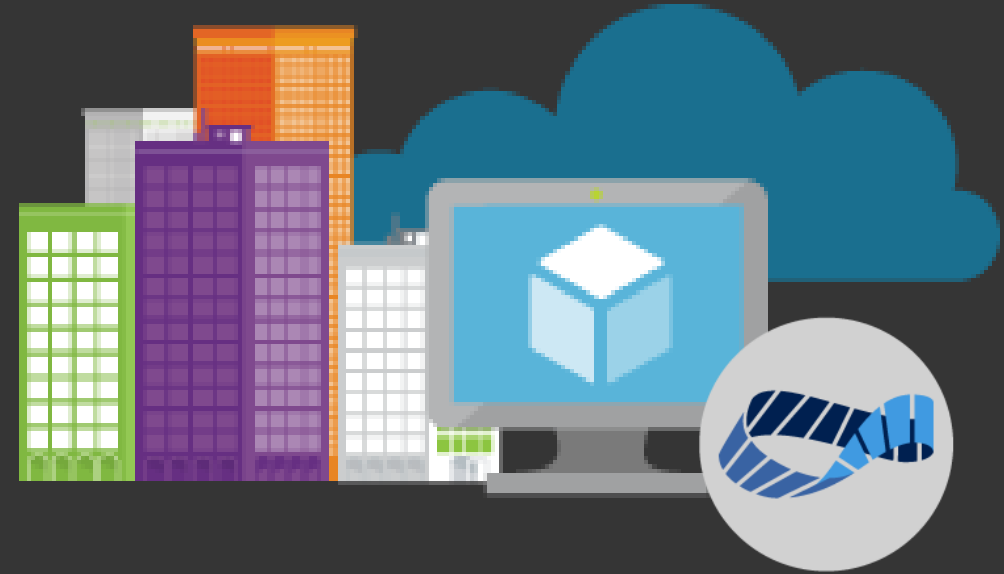


# Applications et Logiciel



# Machines cibles

- **Simulateur à l'état de l'art**
  - Simule 30 qubits dans 16 GB
  - S'exécute localement sur votre PC
- **Simulateur Azure à l'état de l'art**
  - Simule plus que 40 qubits
  - S'exécute dans Azure
- **Simulateur de trace**
  - Détermine les coûts en ressources d'un programme quantique
  - Passe à l'échelle de grands algorithmes et d'un large nombre de qubits
- **Ordinateur Quantique**





Q#

```
using Microsoft.Quantum.Diagnostics;
// Ask for an auxiliary qubit that we can use to prepare
// for teleportation.
let aux = Qubit();

// Create some entanglement that we can use to send
// a message.
CNOT(aux, qubit);
CNOT(qubit, aux);

// Move our message into the entangled pair.
CNOT(qubit, aux);
R(qubit);

// Measure out the entanglement.
if (M(aux) == One) { Z(qubit); }
if (M(qubit) == One) { X(qubit); }
```

# Quantum Development Kit

<https://www.microsoft.com/en-us/quantum/development-kit>

Chiffrement quantique

# Factorisation des nombres et des logarithmes discrets en un temps polynomial

## Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer\*

Peter W. Shor<sup>†</sup>

### Abstract

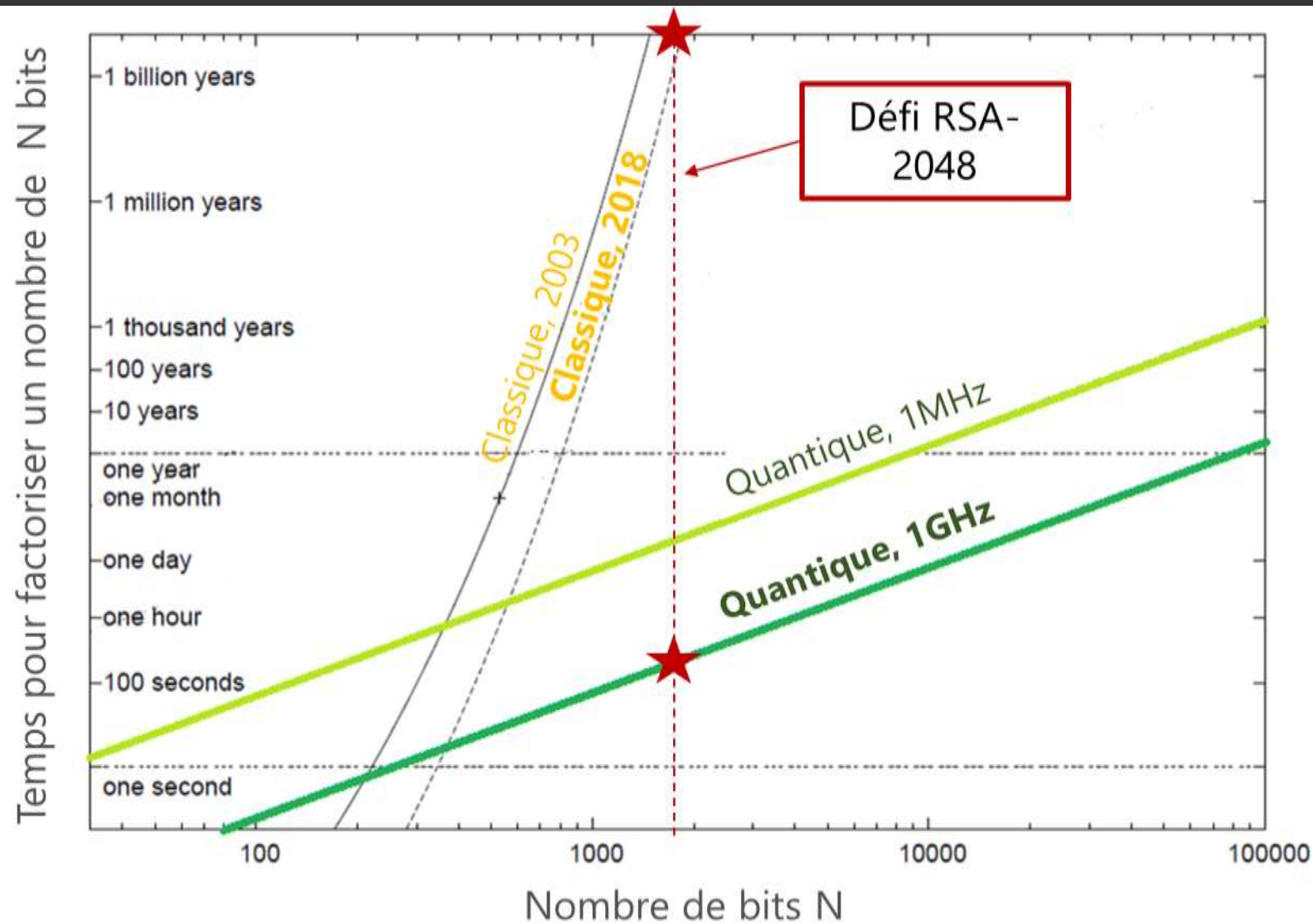
A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

- Factorisation des entiers : RSA est mort !
- Problème de logarithme discret dans les corps finis : DSA est mort !
- Problème de logarithme discret sur les courbes elliptiques : ECDHE est mort !

P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5):1484–1509, 1997. Version antérieure publiée FOCS'94.

<https://arxiv.org/abs/quant-ph/9508027>

# Casser l'algorithme RSA



# Quelle taille d'ordinateur quantique pour casser une clé RSA ?

Microsoft Research a publié récemment un [papier](#) donnant une estimation du nombre de qubits logiques nécessaires pour appliquer l'algorithme de Shor afin de factoriser une clé de chiffrement (RSA et ECC). Les résultats de ce papier sont résumés dans le tableau ci-dessous :

ECDLP in $E(\mathbb{F}_p)$ simulation results					Factoring of RSA modulus $N$ interpolation from [21]		
$\lceil \log_2(p) \rceil$ bits	#Qubits	#Toffoli gates	Toffoli depth	Sim time sec	$\lceil \log_2(N) \rceil$ bits	#Qubits	#Toffoli gates
110	1014	$9.44 \cdot 10^9$	$8.66 \cdot 10^9$	273	512	1026	$6.41 \cdot 10^{10}$
160	1466	$2.97 \cdot 10^{10}$	$2.73 \cdot 10^9$	711	1024	2050	$5.81 \cdot 10^{11}$
192	1754	$5.30 \cdot 10^{10}$	$4.86 \cdot 10^{10}$	1 149	—	—	—
224	2042	$8.43 \cdot 10^{10}$	$7.73 \cdot 10^{10}$	1 881	2048	4098	$5.20 \cdot 10^{12}$
256	2330	$1.26 \cdot 10^{11}$	$1.16 \cdot 10^{11}$	3 848	3072	6146	$1.86 \cdot 10^{13}$
384	3484	$4.52 \cdot 10^{11}$	$4.15 \cdot 10^{11}$	17 003	7680	15362	$3.30 \cdot 10^{14}$
521	4719	$1.14 \cdot 10^{12}$	$1.05 \cdot 10^{12}$	42 888	15360	30722	$2.87 \cdot 10^{15}$

Il ressort de ces travaux qu'il faudrait disposer un budget 2330 qubits logiques pour casser une clé de chiffrement ECC et de 6146 qubits logiques pour casser une clé de chiffrement RSA (une clé ECC 256 bits est l'équivalent d'une clé RSA de 3072 bits).

# Adresser un tel défi

- Il y a trois moyens principaux d'adresser un tel défi qui sont cependant loin d'être parfaits.
  1. Mettre en œuvre une cryptographie dite post-quantique (voir plus loin)
    - L'objectif de cette cryptographie post-quantique est de construire des crypto-systèmes (échange de clef, chiffrement, signature...) capables de résister aux ordinateurs quantiques et donc ne devant pas être remis en cause par l'avènement d'un ordinateur quantique capable de passer à l'échelle.
    - Il existe aujourd'hui plusieurs problèmes, reposant sur différents outils mathématiques, pour lesquels aucun algorithme efficace n'est connu, ni classique, ni quantique.
  2. Utiliser la [cryptographie quantique](#) qui utilise la physique quantique pour concevoir des systèmes cryptographiques plus sécurisés.
    - La principale caractéristique de ces systèmes consiste dans le fait que la mesure d'un état quantique inconnu le perturbera et que de telles perturbations pourront être détectées par les utilisateurs légitimes du système
    - Un tel mécanisme ne fonctionne aujourd'hui pas sur l'Internet existant car il faudrait mettre en place une nouvelle infrastructure de communication mais de telles infrastructures ont déjà été déployées à une échelle plus modeste en promettant une sécurité fondée uniquement sur la physique quantique ainsi que, bien entendu, sur une mise en œuvre appropriée du matériel, par opposition aux problèmes mathématiques qu'un ordinateur quantique (ou tout autre type d'ordinateur) pourrait potentiellement résoudre.

# Adresser un tel défi (suite)

## 1. Utiliser la cryptographie à clé secrète

- C'est-à-dire la cryptographie traditionnelle, où l'expéditeur et le destinataire se rencontrent en secret pour convenir d'une clé, ce qui constitue un mécanisme qui n'est guère menacé par l'informatique quantique.
- Cependant, la cryptographie à clef secrète est également menacée potentiellement par l'irruption de l'ordinateur quantique. Ainsi, l'algorithme de Grover permet une accélération quadratique de la recherche exhaustive
- L'impact d'un ordinateur quantique est ici beaucoup moins important puisqu'il suffit de doubler la taille des clefs en cryptographie symétrique pour se prémunir de l'existence d'un ordinateur quantique.
- Bien que la cryptographie par clé secrète puisse convenir parfaitement aux agences d'espionnage, celle-ci n'est guère pratique pour un déploiement généralisé sur Internet, à moins de disposer également d'un moyen sécurisé pour distribuer les clés.
- C'est précisément pour cela que la cryptographie à clé publique est généralement utilisée aujourd'hui et que la cryptographie quantique pourrait en principe être utilisée à l'avenir : pour échanger des clés privées qui sont ensuite utilisées pour chiffrer et déchiffrer les données réelles.

# Histoire du chiffrement post-quantique

- 2003 : Daniel J. Bernstein introduit le terme « chiffrement post-quantique »
- PQCrypto 2006 : Premier séminaire international sur le chiffrement post-quantique
- PQCrypto 2008, PQCrypto 2010, PQCrypto 2011, PQCrypto 2013
- 2014 : l'UE publie sur programme H2020 qui comprend le chiffrement post-quantique comme l'un des sujets majeurs
- Groupe de travail de l'ETSI sur la « quantum-safe crypto »
- PQCrypto 2014
- Avril 2015 : le NIST héberge un séminaire sur le chiffrement post-quantique
- Août 2015 : la NSA se réveille...





# Annonces de la NSA

- 11 août 2015

*IAD recognizes that there will be a move, in the not distant future, to a quantum resistant algorithm suite.*

- 19 août 2015

*IAD will initiate a transition to quantum resistant algorithms in the not too distant future.*

- La NSA arrive en retard à la fête et bâcle son entrée grandiose...
- *Pire encore maintenant on a des gens qui disent :*
  - « N'utilisez pas la crypto post-quantique, la NSA veut que vous l'utilisiez ! »
  - « La NSA dit que le NIST P-384 (algorithmes ECDSA et ECDH pour une courbe 384 bits) est post-quantum secure »
  - « La NSA a abandonné l'ECC »...

# Le chiffrement post-quantique devient le courant principal

Post-Quantum Cryptography 2016 : 22-26 février à Fukuoka (Japon) > 200 personnes



- Le NIST fait un appel à propositions pour des algorithmes post-quantiques

# Et pendant ce temps, en Europe...

- De même, l'Union Européenne a lancé une initiative sur la cryptographie post-quantique à travers l'investissement auquel a consenti la Commission Européenne qui a investi 3,9 millions d'euros dans le projet [PQCRYPTO](#) lancé en 2015.
- Ce projet a donné lieu à la présentation de [22 propositions](#) lors de la [First Post-Quantum Cryptography Standardization Conference](#) organisée par le NIST en avril dernier.
- Microsoft Research a d'ailleurs présenté [quatre propositions](#) à cette occasion.
- Microsoft Research a également proposé une implémentation en Open Source disponible sur [GitHub](#) d'un fork d'OpenVPN intégré avec du chiffrement post-quantique afin de permettre l'expérimentation de ces algorithmes.

# Quelques algorithmes post-quantiques

- Cryptographie multivariée

- La cryptographie multivariée consiste à construire des crypto-systèmes dont la sécurité repose sur la difficulté du problème PoSSo (*Polynomial System Solving*) : c'est-à-dire de trouver - s'il existe - un zéro commun d'un ensemble de polynômes non-linéaires.
- Le problème PoSSo est NP-difficile et sa difficulté n'est a priori pas remise en cause par l'émergence d'un ordinateur quantique.

- Cryptographie fondée sur les codes correcteurs

- Le cryptosystème de McEliece est le chiffrement à clef publique post-quantique le plus ancien.
- Sa conception date de 1978 ; juste après l'invention de la clef publique par W. Diffie et M. Hellman. La sécurité du crypto-système de McEliece repose sur la difficulté de décoder un code linéaire.
- Revient à trouver la solution d'un système linéaire dont une partie des équations est erronée.
- Il est très simple de résoudre un système d'équations linéaires, mais la tâche est bien plus complexe si les équations comportent des erreurs.
- Ce problème, dénommé *Bounded Distance Decoding*, est notoirement difficile.
- Il a été prouvé NP-Difficile et largement étudié.

# Quelques algorithmes post-quantiques

- Cryptographie fondée sur les réseaux euclidiens
  - Les réseaux euclidiens sont des ensembles périodiques de points de l'espace.
  - Ces structures permettent, entre autres chose, de concevoir des problèmes d'algèbre linéaire pour lesquels, à notre connaissance, aucun algorithme quantique ne permet d'améliorer les algorithmes classiques existants.
  - On trouvera une bonne introduction en français aux réseaux euclidiens en <https://connect.ed-diamond.com/GNU-Linux-Magazine/GLMF-178/Une-cryptographie-nouvelle-le-reseau-euclidien>.
- Pour en savoir plus (cette liste d'algorithmes est loin d'être exhaustive)
  - Si vous êtes intéressé par les aspects mathématiques liés au chiffrement post-quantique il est possible de consulter avec intérêt la [thèse en français](#) « Contributions à la cryptographie post-quantique ».

# Le problème avec cette approche

- Le problème avec de tels systèmes post-quantiques est qu'ils ont été à peine testés.
  - On ignore encore à ce jour si le problème de la factorisation – contrairement à une idée trop souvent répandue – est NP-complet et on n'a même aucune raison de penser qu'il le soit... mais au moins une preuve tangible que ce problème est difficile est que de nombreux mathématiciens pointus ont essayé pendant des décennies de trouver des algorithmes de factorisation performants et ont échoué.
- Les problèmes de calcul alternatifs suggérés pour la cryptographie post-quantique n'ont pas encore fait l'objet d'un tel examen et il pourrait bien exister un algorithme quantique (ou même classique !) efficace capable de les casser.
  - Ainsi, si de nombreuses solutions théoriques existent, il reste à faire aboutir les travaux de recherche en cours afin de déboucher sur des solutions concrètes.
- C'est la raison pour laquelle des initiatives ont été lancées depuis quelques années afin de stimuler la recherche sur ce sujet de la cryptographie post-quantique

# L'importance et l'urgence du sujet...

- Brian La Macchia, qui dirige l'ensemble des activités de Microsoft Research en la matière, a récemment enregistré un [podcast](#) sur ce sujet.
- Son point de vue sur l'importance du sujet et son urgence est clair :  
*« so the thing that keeps me up at night is that, say Krysta Svore and her team are going to be successful sooner rather than later. And by that, I mean that we're going to see quantum computers show up more quickly than we anticipate, that the qubit construction challenges and the scaling problems will get solved by the very smart people working on them faster than we can standardize and deploy defenses. There's this arms race going on between the quantum computing folks who are trying to build the quantum computers, and the post-quantum cryptographers trying to make sure the defenses are out there before the quantum computing people are successful. That's what keeps me up at night, but it's a good problem to have. »*

# L'importance et l'urgence du sujet...

- Aujourd'hui, qu'on le veuille ou non, le risque de l'ordinateur quantique est perçu par la communauté de la sécurité comme très élevé.
- Ne serait-ce que pour la possibilité de voir des données chiffrées et stockées le temps qu'un ordinateur suffisamment puissant (quantique) puisse les déchiffrer.
- C'est notamment le cas des secrets ayant par nature une longue durée de vie – par exemple les données gouvernementales classifiées et les données médicales – pour lesquelles cette menace est jugée crédible.
  - L'[ETSI](#) a ainsi publié la liste des blocs de base des infrastructures IT « à risque ».



# L'importance et l'urgence du sujet...

- Dans le mesure où
  - (1) il y a encore pas mal de recherches à faire sur le sujet afin de s'assurer de la solidité des algorithmes post-quantiques,
  - (2) le déploiement d'un nouveau standard cryptographique au niveau mondial prendra nécessairement du temps, probablement plus d'une dizaine d'années
  - (3) l'implémentation et l'interaction des composantes post-quantiques avec des protocoles de plus haut niveau comme TLS, SSH et IPsec risque également d'avoir quelques bogues à moins que l'on n'arrive à la mise en place d'une implémentation prouvée de ces briques.
- C'est la raison pour laquelle le NIST, l'ETSI et d'autres institutions internationales et nationales, estiment qu'il est nécessaire d'agir dès maintenant pour évoluer vers la mise en œuvre d'algorithmes post-quantiques.

HOW'S YOUR  
QUANTUM COMPUTER  
PROTOTYPE COMING  
ALONG?

GREAT!



THE PROJECT EXISTS  
IN A SIMULTANEOUS  
STATE OF BEING BOTH  
TOTALLY SUCCESSFUL  
AND NOT EVEN  
STARTED.



CAN I  
OBSERVE  
IT?

THAT'S  
A TRICKY  
QUESTION.



Dilbert.com DilbertCartoonist@gmail.com

4-17-12 ©2012 Scott Adams, Inc. /Dist. by Universal Uclick

# Q&A

