Rapport Approfondi sur l'Informatique Quantique : Fondements, État Actuel et Perspectives

---

Chapitre 1 : Document d'Information

Introduction

L'informatique quantique est un domaine émergent de l'informatique qui exploite les principes fondamentaux de la mécanique quantique pour résoudre des problèmes d'une complexité hors de portée, même pour les supercalculateurs classiques les plus puissants. En s'appuyant sur des phénomènes contre-intuitifs tels que la superposition et l'intrication, cette technologie promet de révolutionner des secteurs allant de la découverte de médicaments à la science des matériaux, en passant par la finance et la cybersécurité. Son importance stratégique est aujourd'hui reconnue mondialement, suscitant un enthousiasme et des investissements considérables de la part des gouvernements, des institutions académiques et des géants de l'industrie. Ce rapport se propose d'analyser en profondeur les fondements de l'informatique quantique, son état actuel et les perspectives qu'elle ouvre.

1.1. Résumé Exécutif

Cette analyse synthétise les points critiques de l'informatique quantique, révélant un domaine à la fois prometteur et confronté à des défis techniques majeurs.

- **Principes Fondamentaux :** La puissance de calcul quantique repose sur la **superposition** (un qubit peut être 0, 1, ou les deux à la fois), l'**intrication** (des qubits sont liés de manière non locale), l'**interférence** (pour amplifier les bons résultats) et la **mesure** (qui fige le résultat dans un état classique).
- **Architectures Dominantes :** Deux paradigmes coexistent. L'**informatique quantique à base de portes** est un modèle universel, capable d'exécuter des algorithmes comme ceux de Shor et Grover. Le **recuit quantique**, plus spécialisé, est conçu pour les problèmes d'optimisation.
- **Défis Majeurs :** La technologie est actuellement dans l'ère **NISQ (Noisy Intermediate-Scale Quantum)**. Les principaux obstacles sont la **décohérence** (la perte de l'état quantique due au bruit environnemental), les **taux d'erreur** élevés et la **difficulté de mise à l'échelle** (scalabilité). La **Correction d'Erreurs Quantiques (QEC)** est essentielle pour surmonter ces défis.
- **Applications Potentielles :** Les domaines les plus prometteurs incluent la **chimie et la science des matériaux** (simulation de molécules), la **finance** (optimisation de portefeuilles), l'**intelligence artificielle** (IA quantique) et la **cryptographie**, où l'algorithme de Shor menace les systèmes actuels, stimulant le développement de la cryptographie post-quantique (PQC).
- **Trajectoire Future :** Des acteurs majeurs comme IBM et Google mènent la course. La feuille de route d'**IBM**, par exemple, vise à atteindre un **"avantage quantique"** (résoudre un problème pratique mieux qu'un ordinateur classique) d'ici 2026 et à construire un ordinateur tolérant aux pannes d'ici 2029, marquant la transition de la recherche fondamentale vers des applications concrètes.

1.2. Les Principes Fondamentaux de la Mécanique Quantique

La puissance de l'informatique quantique découle directement de quatre principes de la mécanique quantique qui régissent le comportement de la matière à l'échelle atomique et subatomique.

- **Superposition** La superposition est la capacité d'un système quantique, comme un qubit, à exister dans une combinaison de plusieurs états simultanément. Contrairement à un bit classique qui ne peut être que 0 ou 1, un qubit peut être 0, 1, ou les deux à la fois. Cette propriété permet aux ordinateurs quantiques de traiter de vastes combinaisons d'entrées en parallèle. En explorant simultanément une multitude de possibilités, les ordinateurs quantiques peuvent résoudre certains problèmes complexes de manière exponentiellement plus rapide que les ordinateurs classiques.
- **Intrication** L'intrication est un phénomène où deux ou plusieurs qubits deviennent si profondément corrélés que leur état collectif ne peut être décrit indépendamment. La mesure de l'état d'un qubit intriqué affecte instantanément l'état des autres, quelle que soit la distance qui les sépare. Cette connexion non locale est une ressource cruciale qui augmente la puissance de traitement, permet des calculs complexes sur plusieurs qubits et joue un rôle fondamental dans les stratégies de correction d'erreurs quantiques.
- **Interférence** L'interférence est le mécanisme par lequel les algorithmes quantiques guident les calculs vers la bonne solution. Les états des qubits se comportent comme des ondes, avec des amplitudes de probabilité. Les algorithmes sont conçus pour que les chemins de calcul menant aux résultats corrects interfèrent de manière constructive (leurs amplitudes s'additionnent), tandis que ceux menant à des résultats incorrects interfèrent de manière destructive (leurs amplitudes s'annulent). Ce processus permet d'amplifier la probabilité de mesurer la solution souhaitée.
- **Mesure** La mesure est l'acte final d'un calcul quantique. Lorsqu'un qubit en superposition est mesuré, son état quantique s'effondre et il est forcé de prendre un état classique défini, soit 0, soit 1. Le résultat de la mesure est probabiliste, déterminé par les amplitudes de la superposition juste avant la mesure. L'interférence a pour but de maximiser la probabilité que cette mesure donne le résultat correct.

Ces principes sont mis en œuvre différemment selon les architectures matérielles et les modèles de calcul, qui définissent les capacités et les limites des ordinateurs quantiques actuels.

1.3. Architectures Quantiques et Implémentations Physiques

Deux paradigmes principaux dominent le paysage de l'informatique quantique. Le premier, l'**informatique quantique à base de portes**, est un modèle de calcul universel. Le second, le **recuit quantique**, est une approche plus spécialisée. Le recuit quantique se divise lui-même en deux catégories : le Recuit Quantique Analogique (AQA), qui repose sur l'évolution continue d'un système physique, et le Recuit Quantique Numérique (DQA), qui utilise le modèle de circuits à base de portes pour simuler le processus de recuit.

Caractéristique	Informatique Quantique à base de Portes (Gate-Based)	Recuit Quantique Analogique (AQA)
Modèle de Calcul	Universel. Utilise des circuits de portes quantiques pour exécuter une large gamme d'algorithmes.	Spécialisé. Conçu pour résoudre des problèmes d'optimisation en trouvant l'état d'énergie minimal d'un système quantique.
Algorithmes	Algorithmes comme Shor (factorisation) et Grover (recherche). Sert aussi de base pour le DQA, comme le QAOA (Quantum Approximate Optimization Algorithm).	Algorithme Adiabatique Quantique (QAA), exploitant l'évolution naturelle du système.
Sensibilité au Bruit	Très sensible à la décohérence et aux erreurs. Nécessite une correction d'erreurs quantiques (QEC) robuste pour des calculs à grande échelle.	Moins sensible à certains types d'erreurs car il exploite la tendance naturelle du système à trouver son état de plus basse énergie.

Pour construire physiquement ces ordinateurs, les chercheurs explorent diverses technologies pour créer des qubits, chacune ayant ses propres avantages et inconvénients.

- **Qubits Supraconducteurs** Ce sont des circuits électriques fabriqués à partir de matériaux supraconducteurs qui doivent être maintenus à des températures cryogéniques. Ils sont rapides et leur fabrication s'appuie sur des techniques de semi-conducteurs existantes. C'est l'approche privilégiée par des entreprises comme IBM et Google.
- **Qubits à Ions Piégés** Ces qubits utilisent des atomes chargés (ions) piégés dans des champs électromagnétiques. Ils sont remarquables pour leur grande stabilité et leurs longs temps de cohérence, mais les opérations de portes sont généralement plus lentes. Cette technologie est développée par des entreprises comme IonQ et Honeywell.
- **Qubits Photoniques** Ils utilisent des particules de lumière (photons) comme qubits. L'information peut être encodée dans la polarisation du photon. Les photons sont très résistants au bruit et idéaux pour la communication quantique, mais la création de portes à deux qubits est un défi.
- **Points Quantiques (Quantum Dots)** Il s'agit de minuscules semi-conducteurs qui piègent un seul électron. Le spin de l'électron est utilisé comme qubit. Cette technologie offre un potentiel de scalabilité élevé et une bonne compatibilité avec les technologies de fabrication existantes.
- **Centres Azote-Lacune (NV) dans le Diamant** Ces systèmes utilisent les défauts cristallins dans les diamants, où un atome de carbone est remplacé par un atome d'azote à côté d'une lacune, pour piéger des électrons dont les états de spin servent de qubits. Ils sont stables à température ambiante, ce qui constitue un avantage notable.
- **Atomes** Les atomes neutres peuvent également être utilisés comme qubits, en stockant l'information dans leurs niveaux d'énergie. Ils sont très stables et moins sensibles au bruit, ce qui permet de réaliser des calculs de longue durée.

Malgré la diversité de ces approches, tous les systèmes quantiques sont confrontés à un ensemble commun de défis fondamentaux liés à la fragilité de l'état quantique, qui doivent être surmontés pour atteindre une informatique quantique à grande échelle et tolérante aux pannes.

1.4. L'Ère NISQ et les Défis de l'Informatique Quantique

L'état actuel de la technologie est défini par l'ère des **"Noisy Intermediate-Scale Quantum (NISQ)"**. Ce terme décrit des ordinateurs quantiques qui possèdent un nombre intermédiaire de qubits (de 50 à quelques milliers) mais qui sont encore trop "bruyants" et sujets aux erreurs pour exécuter des algorithmes complexes nécessitant une correction d'erreurs complète. La gestion de ces erreurs est le défi stratégique central pour faire progresser le domaine.

Trois défis majeurs entravent les progrès :

1. **Décohérence** La décohérence est le processus par lequel les qubits perdent leur état quantique (superposition et intrication) en raison d'interactions non désirées avec leur environnement, telles que les fluctuations de température, les vibrations ou les interférences électromagnétiques. Ce phénomène limite la durée pendant laquelle un calcul quantique peut être effectué de manière fiable avant que l'information ne soit corrompue.

2. **Taux d'Erreur** Les opérations quantiques ne sont pas parfaites. Divers types d'erreurs peuvent survenir : les erreurs de bit (bit-flip, où $|0\rangle$ devient $|1\rangle$ et vice-versa), les erreurs de phase (phase-flip, où $|1\rangle$ devient $-|1\rangle$), les erreurs de porte, où une opération n'est pas appliquée avec une précision parfaite, et la diaphonie (crosstalk), où une opération sur un qubit affecte involontairement ses voisins. L'impact de ces erreurs est cumulatif et peut rapidement rendre un calcul complexe inutilisable.

3. **Scalabilité** Augmenter le nombre de qubits dans un processeur est un défi de taille. Il ne suffit pas d'ajouter des qubits ; il faut également maintenir un contrôle précis sur chacun d'eux, assurer une connectivité suffisante entre eux pour permettre des opérations d'intrication, et les isoler efficacement du bruit environnemental.

La solution à long terme pour surmonter ces défis est la **Correction d'Erreurs Quantiques (QEC)**. La QEC est un ensemble de techniques visant à détecter et corriger les erreurs dans les qubits sans mesurer directement et donc détruire leur état quantique. Contrairement à la correction d'erreurs classique, qui repose sur la redondance en copiant les bits, la QEC est plus complexe en raison du **théorème de non-clonage**, qui interdit de faire une copie parfaite d'un état quantique inconnu. L'objectif ultime de la maîtrise de la QEC est de faire la transition de l'ère NISQ vers l'informatique quantique tolérante aux pannes (Fault-Tolerant Quantum Computing - FTQC), un jalon clé de la feuille de route d'IBM, prévu pour 2029. Ce n'est qu'en atteignant cet objectif que des applications révolutionnaires pourront être mises en œuvre de manière fiable.

1.5. Applications, Avantage Quantique et Écosystème

La promesse ultime de l'informatique quantique est de résoudre des problèmes pratiques aujourd'hui insolubles, en offrant des solutions plus rapides, plus précises ou plus économiques que n'importe quelle méthode classique.

Pour comprendre la trajectoire du domaine, il est crucial de distinguer deux concepts clés. La **Suprématie Quantique**, démontrée par Google en 2019, est une étape de recherche fondamentale où un ordinateur quantique effectue une tâche spécifique — même sans utilité pratique — plus

rapidement qu'un supercalculateur classique. En revanche, l'**Avantage Quantique** est l'objectif commercial et pratique : utiliser un ordinateur quantique pour résoudre un problème du monde réel de manière plus efficace (en termes de temps, de coût ou de qualité de la solution) que la meilleure alternative classique connue.

Les domaines d'application les plus prometteurs pour atteindre cet avantage quantique sont les suivants :

- **Chimie et Science des Matériaux** Les ordinateurs quantiques peuvent simuler le comportement des molécules et des matériaux au niveau quantique avec une précision inaccessible aux ordinateurs classiques. Cela pourrait accélérer radicalement la découverte de nouveaux médicaments, la conception de matériaux plus performants et l'optimisation de catalyseurs industriels.
- **Finance** Dans le secteur financier, les algorithmes quantiques pourraient être utilisés pour des tâches d'optimisation complexes, telles que la gestion de portefeuilles d'investissement, la modélisation des marchés pour évaluer les risques, ou la tarification d'instruments financiers dérivés.
- **Apprentissage Automatique (IA Quantique)** L'informatique quantique a le potentiel d'accélérer certains algorithmes d'apprentissage automatique. L'IA quantique pourrait améliorer l'analyse de grands ensembles de données, la reconnaissance de formes et la résolution de problèmes d'optimisation au cœur de l'intelligence artificielle.
- **Cryptographie** L'informatique quantique présente à la fois une menace et une opportunité pour la cybersécurité. L'**algorithme de Shor** est capable de casser les systèmes de cryptographie à clé publique actuels (comme RSA). Cette menace a conduit à l'émergence de la **cryptographie post-quantique (PQC)**, qui développe de nouveaux algorithmes de chiffrement résistants aux attaques des ordinateurs classiques et quantiques.

L'écosystème de l'informatique quantique est en pleine expansion, mené par des entreprises comme **IBM, Google, D-Wave, Rigetti, Xanadu, Infleqtion, IonQ** et **Honeywell**. IBM, par exemple, a une feuille de route ambitieuse visant à démontrer un premier "avantage quantique" d'ici 2026 et à construire un ordinateur quantique tolérant aux pannes en 2029. Le domaine est à un point d'inflexion, passant d'une phase de recherche purement académique à une ère où les applications pratiques deviennent une réalité tangible.

Chapitre 2 : Guide d'Étude

Introduction

Ce chapitre est conçu comme un outil pour consolider votre compréhension des concepts clés de l'informatique quantique présentés dans ce rapport. À travers un quiz, des questions de réflexion et un glossaire des termes essentiels, ce guide vise à renforcer l'apprentissage et à encourager une analyse plus approfondie des enjeux et des technologies qui façonnent ce domaine révolutionnaire.

2.1. Quiz : Questions à Réponse Courte

1. Quelle est la différence fondamentale entre un bit classique et un qubit ?

2. Expliquez brièvement le principe de la superposition quantique.
3. Qu'est-ce que l'intrication quantique et pourquoi est-elle importante ?
4. Quels sont les deux principaux paradigmes de l'informatique quantique décrits dans les sources ?
5. Qu'est-ce que la décohérence et quel est son principal impact sur les calculs quantiques ?
6. Définissez le terme "NISQ" (Noisy Intermediate-Scale Quantum).
7. Pourquoi les techniques de correction d'erreurs classiques ne peuvent-elles pas être directement appliquées aux ordinateurs quantiques ?
8. Citez deux applications potentielles de l'informatique quantique.
9. Quelle est la différence entre la "suprématie quantique" et l'"avantage quantique" ?
10. Nommez deux types de qubits physiques utilisés pour construire des ordinateurs quantiques.

2.2. Corrigé du Quiz

1. Un bit classique ne peut avoir qu'une seule valeur à la fois, soit 0, soit 1. Un qubit, grâce à la superposition, peut exister dans un état de 0, 1, ou une combinaison des deux simultanément, ce qui augmente considérablement la capacité de traitement de l'information.
2. La superposition quantique est le principe selon lequel un qubit peut exister dans une combinaison de tous ses états possibles en même temps. Cela permet à un ordinateur quantique d'explorer de multiples possibilités simultanément, accélérant la résolution de problèmes complexes.
3. L'intrication est une corrélation profonde entre plusieurs qubits, où l'état d'un qubit est instantanément lié à celui des autres, quelle que soit la distance. Elle est cruciale pour la puissance de calcul et pour la mise en œuvre de la correction d'erreurs quantiques.
4. Les deux principaux paradigmes sont l'informatique quantique à base de portes (un modèle universel pour divers algorithmes comme Shor) et le recuit quantique (un modèle spécialisé pour les problèmes d'optimisation).
5. La décohérence est la perte de l'état quantique d'un qubit en raison d'interactions avec son environnement (bruit, température). Son principal impact est de limiter la durée des calculs et d'introduire des erreurs, rendant les calculs peu fiables.
6. "NISQ" désigne l'ère actuelle des ordinateurs quantiques, qui sont de taille intermédiaire mais encore trop "bruyants" (sujets aux erreurs) pour exécuter des algorithmes complexes nécessitant une correction d'erreurs complète.
7. Les techniques classiques reposent sur la copie de l'information pour créer de la redondance. Le théorème de non-clonage en mécanique quantique interdit de créer une copie parfaite d'un état quantique inconnu, ce qui rend cette approche inapplicable.

8. Deux applications potentielles sont la découverte de médicaments grâce à la simulation moléculaire et l'optimisation de portefeuilles financiers pour une meilleure gestion des risques.
9. La "suprématie quantique" est la démonstration qu'un ordinateur quantique peut effectuer une tâche (même inutile) plus rapidement qu'un supercalculateur. L'"avantage quantique" est la capacité de résoudre un problème pratique et réel mieux qu'un ordinateur classique.
10. Deux types de qubits physiques sont les qubits supraconducteurs (utilisés par IBM et Google) et les qubits à ions piégés (utilisés par IonQ et Honeywell).

2.3. Questions de Réflexion (Format Essai)

1. Discutez des principaux défis techniques (décohérence, taux d'erreur, scalabilité) qui entravent le développement d'ordinateurs quantiques tolérants aux pannes à grande échelle, et analysez le rôle de la Correction d'Erreurs Quantiques (QEC) pour surmonter ces obstacles.
2. Comparez et contrastez l'informatique quantique à base de portes (gate-based) et le recuit quantique (quantum annealing) en termes de modèle de calcul, d'applications typiques et de défis de mise en œuvre.
3. Analysez l'impact potentiel de l'algorithme de Shor sur la cybersécurité mondiale et expliquez l'importance et les approches de la cryptographie post-quantique (PQC).
4. Évaluez le débat sur la menace existentielle posée par l'intelligence artificielle (IA) combinée à l'informatique quantique, en vous basant sur les arguments présentés dans le fil de discussion Reddit.
5. En vous appuyant sur les feuilles de route et les avancées mentionnées par des entreprises comme IBM, décrivez la trajectoire probable de l'informatique quantique au cours de la prochaine décennie, de "l'utilité quantique" à "l'avantage quantique".

2.4. Glossaire des Termes Clés

- **Algorithme de Grover :** Un algorithme quantique qui peut rechercher dans une base de données non triée de manière quadratiquement plus rapide que n'importe quel algorithme classique.
- **Algorithme de Shor :** Un algorithme quantique qui peut factoriser de grands nombres de manière exponentiellement plus rapide que n'importe quel algorithme classique connu, menaçant la cryptographie actuelle.
- **Avantage Quantique :** Situation où un ordinateur quantique peut fournir une solution meilleure, plus rapide ou moins chère qu'une méthode classique pour un problème pratique et réel.
- **Bit Classique :** L'unité d'information fondamentale de l'informatique classique, qui ne peut prendre que deux valeurs possibles : 0 ou 1.
- **Circuit Quantique :** Une séquence de portes quantiques appliquées à des qubits. C'est l'équivalent quantique d'un circuit logique classique.

- **Correction d'Erreurs Quantiques (QEC) :** Un ensemble de techniques visant à détecter et corriger les erreurs dans les qubits sans détruire leur état quantique, essentiel pour construire des ordinateurs quantiques fiables.
- **Cryptographie Post-Quantique (PQC) :** Des algorithmes cryptographiques conçus pour être sécurisés contre les attaques d'ordinateurs classiques et quantiques.
- **Décohérence :** Le processus par lequel les qubits perdent leurs propriétés quantiques (comme la superposition) en raison d'interactions avec leur environnement, ce qui introduit des erreurs dans les calculs.
- **Intrication :** Un phénomène quantique où les états de plusieurs qubits sont si profondément liés que l'état d'un seul ne peut être décrit sans décrire les autres, quelle que soit la distance qui les sépare.
- **NISQ (Noisy Intermediate-Scale Quantum) :** Terme décrivant l'ère actuelle des ordinateurs quantiques, qui ont une taille intermédiaire mais sont encore trop "bruyants" (sujets aux erreurs) pour des calculs complexes tolérants aux pannes.
- **Porte Quantique :** L'équivalent quantique d'une porte logique classique. Ce sont les briques de base des algorithmes quantiques, utilisées pour manipuler l'état des qubits.
- **Qubit :** L'unité d'information fondamentale de l'informatique quantique. Il peut exister dans un état de 0, 1, ou une superposition des deux simultanément.
- **Recuit Quantique (Quantum Annealing) :** Un paradigme d'informatique quantique spécialisé dans la résolution de problèmes d'optimisation en exploitant la tendance naturelle des systèmes quantiques à trouver leur état d'énergie le plus bas.
- **Superposition :** Le principe quantique qui permet à un qubit d'exister dans une combinaison de plusieurs états à la fois (0 et 1), augmentant ainsi la puissance de calcul.
- **Suprématie Quantique :** Une démonstration expérimentale où un ordinateur quantique effectue une tâche spécifique plus rapidement que le supercalculateur classique le plus puissant, indépendamment de l'utilité pratique de la tâche.

Chapitre 3 : Foire Aux Questions (FAQ)

Introduction

Cette section répond aux dix questions les plus fréquemment posées sur l'informatique quantique. Les réponses sont formulées pour être claires et accessibles, en s'appuyant exclusivement sur les thèmes et les informations abordés dans les documents sources de ce rapport.

3.1. Questions et Réponses

1. **Q : Qu'est-ce que l'informatique quantique en termes simples ? R :** L'informatique quantique est une nouvelle façon de calculer qui utilise les lois de la physique quantique. Au lieu d'utiliser des bits classiques (0 ou 1), elle utilise des "qubits" qui peuvent être 0, 1, ou les deux en même temps grâce à un principe appelé superposition. En exploitant ce phénomène ainsi que l'intrication, les ordinateurs quantiques peuvent explorer un très grand nombre de possibilités simultanément, ce qui leur permet de résoudre certains

problèmes extrêmement complexes beaucoup plus rapidement que les ordinateurs classiques.

2. **Q : L'informatique quantique va-t-elle remplacer les ordinateurs classiques ? R :** Non, l'informatique quantique ne remplacera pas les ordinateurs classiques. Les ordinateurs classiques resteront supérieurs pour la grande majorité des tâches quotidiennes. Les ordinateurs quantiques sont des machines hautement spécialisées, conçues pour s'attaquer à des types de problèmes spécifiques (comme la simulation moléculaire ou l'optimisation complexe) qui sont insolubles pour les machines classiques. À l'avenir, ils travailleront probablement en tandem avec des supercalculateurs classiques dans des systèmes hybrides.

3. **Q : Quel est le plus grand défi de l'informatique quantique aujourd'hui ? R :** Le plus grand défi est la fragilité des qubits et la gestion des erreurs. Les qubits sont extrêmement sensibles à leur environnement (bruit, température), ce qui provoque un phénomène appelé "décohérence" où ils perdent leur état quantique. Cela conduit à des taux d'erreur élevés qui rendent les calculs peu fiables. La construction de systèmes capables de corriger ces erreurs en temps réel est l'obstacle majeur à surmonter pour construire des ordinateurs quantiques à grande échelle.

4. **Q : Comment fonctionnent les qubits ? R :** Les qubits sont les unités d'information de base des ordinateurs quantiques. Contrairement aux bits classiques, ils peuvent exister dans un état de 0, 1, ou une superposition des deux. Ils sont créés physiquement en utilisant diverses technologies, telles que des circuits électriques supraconducteurs refroidis à des températures extrêmement basses, des ions individuels piégés par des champs électromagnétiques, ou des particules de lumière (photons). Des impulsions de micro-ondes ou de lasers sont utilisées pour manipuler leur état et effectuer des calculs.

5. **Q : Qu'est-ce que la Correction d'Erreurs Quantiques (QEC) ? R :** La Correction d'Erreurs Quantiques (QEC) est un ensemble de techniques conçues pour détecter et corriger les erreurs qui se produisent dans les qubits sans mesurer directement leur état (ce qui le détruirait). Elle fonctionne en encodant l'information d'un qubit "logique" sur plusieurs qubits "physiques" redondants. En surveillant ces qubits physiques, il est possible de détecter quand une erreur s'est produite et de la corriger, rendant ainsi les calculs quantiques plus fiables et tolérants aux pannes.

6. **Q : Quelles sont les applications concrètes de l'informatique quantique ? R :** Les applications concrètes incluent la découverte de nouveaux médicaments et matériaux en simulant précisément le comportement des molécules, l'optimisation dans la finance pour créer des portefeuilles d'investissement plus performants, et l'amélioration de l'intelligence artificielle en accélérant certains algorithmes d'apprentissage automatique. D'autres applications concernent la logistique, la modélisation climatique et la cybersécurité.

7. **Q : L'informatique quantique représente-t-elle une menace pour la sécurité des données ? R :** Oui, elle représente une menace significative. L'algorithme de Shor, exécutable sur un ordinateur quantique suffisamment puissant, peut casser les systèmes de cryptographie à clé publique (comme RSA) qui protègent actuellement la plupart de nos communications et transactions en ligne. Pour contrer cette menace, les chercheurs développent la Cryptographie Post-Quantique (PQC), qui consiste en de nouveaux

algorithmes de chiffrement conçus pour résister aux attaques des ordinateurs classiques et quantiques.

8. **Q : Qu'est-ce que Qiskit ? R :** Qiskit est un kit de développement logiciel (SDK) open-source créé par IBM. Il permet aux développeurs, aux chercheurs et aux étudiants de programmer des ordinateurs quantiques. Qiskit offre des outils pour créer et manipuler des circuits quantiques, exécuter des algorithmes sur de vrais ordinateurs quantiques ou des simulateurs via le cloud, et explorer des applications dans divers domaines.
9. **Q : Peut-on acheter un ordinateur quantique ? R :** Il n'est généralement pas possible pour un particulier ou une entreprise d'acheter un ordinateur quantique universel comme on achète un ordinateur portable. Ces machines sont extrêmement complexes, coûteuses et nécessitent des conditions environnementales extrêmes. L'accès à l'informatique quantique se fait principalement via des plateformes cloud, comme IBM Quantum ou Amazon Braket, qui permettent aux utilisateurs d'exécuter leurs algorithmes sur du matériel quantique à distance.
10. **Q : Quand verrons-nous l' "avantage quantique" ? R :** Selon la feuille de route d'IBM, l'avantage quantique — le moment où un ordinateur quantique pourra résoudre un problème pratique de manière plus efficace (meilleure, plus rapide ou moins chère) que n'importe quelle méthode classique — est attendu d'ici 2026. Cela marquera une étape cruciale où l'informatique quantique commencera à avoir un impact commercial et scientifique tangible.

Chapitre 4 : Chronologie

Introduction

Cette section présente une chronologie des étapes et des percées significatives qui ont jalonné le développement de l'informatique quantique et de la correction d'erreurs. Basée sur les dates clés extraites des sources, elle retrace le parcours de ce domaine, depuis les idées théoriques initiales jusqu'aux feuilles de route ambitieuses d'aujourd'hui.

4.1. Chronologie des Développements Clés

- **1982 :** Richard Feynman propose l'idée d'une machine quantique capable de simuler la physique quantique, jetant les bases conceptuelles de l'informatique quantique.
- **1994 :** Peter Shor publie son algorithme de factorisation, démontrant une application puissante et révolutionnaire pour un futur ordinateur quantique, capable de briser la cryptographie moderne.
- **1995 :** Peter Shor propose le premier schéma de correction d'erreurs quantiques (le code de Shor à 9 qubits), une étape fondamentale pour rendre les calculs quantiques fiables.
- **1996 :** Andrew Steane propose un code QEC à sept qubits plus efficace (le code de Steane), améliorant l'efficience de la correction d'erreurs.
- **1997 :** Alexei Kitaev introduit les codes topologiques, une nouvelle approche robuste pour la QEC qui est moins sensible aux erreurs locales.

- **2002 :** Le "code de surface" est proposé par E. Dennis, A. Kitaev, A. Landahl et J. Preskill, devenant l'un des candidats les plus prometteurs pour la construction d'ordinateurs quantiques tolérants aux pannes.
- **2006 :** Introduction des codes "Bacon-Shor" et des "codes couleur 3D", élargissant le champ des techniques de correction d'erreurs quantiques.
- **2016 :** IBM rend un processeur quantique de 5 qubits accessible au public via le cloud (IBM Quantum Experience), démocratisant l'accès à la technologie et stimulant l'expérimentation.
- **2019 :** Google annonce avoir atteint la "suprématie quantique" avec son processeur Sycamore, démontrant qu'un ordinateur quantique peut surpasser un supercalculateur classique sur une tâche spécifique.
- **2023 :** IBM démontre "l'utilité quantique", montrant que ses ordinateurs quantiques peuvent produire des solutions précises à des problèmes au-delà de ce que la simulation classique par force brute peut atteindre.
- **2026 (Perspective) :** IBM prévoit d'atteindre le premier "avantage quantique", où un ordinateur quantique résoudra un problème pratique de manière plus efficace que toute méthode classique.
- **2029 (Perspective) :** IBM vise la construction d'un ordinateur quantique tolérant aux pannes à grande échelle, une étape majeure vers la pleine réalisation du potentiel de la technologie.

Chapitre 5 : Liste des Sources

Introduction

Cette section répertorie les documents académiques, les articles et les pages web qui ont servi de base à l'élaboration de ce rapport. Les références sont formatées selon une norme scientifique afin de garantir la traçabilité et la crédibilité des informations présentées.

5.1. Références Scientifiques

- AbuGhanem, M. & Eleuch, H. (2024). Two-qubit entangling gates for superconducting quantum computers. *Results in Physics*, 56, 107236.
- Aharonov, D., Van Dam, W., Kempe, J., Landau, Z., Lloyd, S., & Regev, O. Adiabatic Quantum Computation Is Equivalent To Standard Quantum Computation. *SIAM Journal On Computing*, 37, 166-194.
- Albash, T. & Lidar, D. A. (2018). Adiabatic quantum computation. *Reviews of Modern Physics*, 90(1), 015002.
- Albash, T., et al. (2015). Dynamics Of A Quantum Phase Transition. *Physical Review A*, 92, 042321.
- Albash, T., Lidar, D. A., Martonosi, M., & Roetteler, M. (2018). Demonstrating The Robustness Of A Hybrid Quantum Annealer. *Physical Review X*, 8, 031016.

- Albash, T., Lidar, D. A., Martoňák, R., & Zanardi, P. (2018). Colloquium: Quantum Annealing And Analog Quantum Computation. *Reviews Of Modern Physics*, 90, 021001.
- Albash, T., Martin-mayor, V., Hen, I., & Troyer, M. (2018). Temperature Scaling Of The Quantum Annealing Performance. *Physical Review A*, 98, 022313.
- Amin, M. H., Andriyash, E., Rolfe, J., Kulczycki, B., & Melko, R. (2015). Quantum Boltzmann Machines. *Physical Review X*, 5, 031011.
- Amin, M. H. S., Love, P. J., & Truncik, C. J. S. (2009). Dynamical Suppression Of Decoherence In Two-state Quantum Systems. *Physical Review Letters*, 103, 260503.
- Amin, M. H., Love, P. J., & Truncik, C. J. S. (2009). Thermally Assisted Adiabatic Quantum Computation. *Physical Review Letters*, 103, 260503.
- Aramon, M., Rosenberg, G., Valiante, E., Miyazawa, T., Tamura, H., & Katzgraber, H. G. (2019). Physics-inspired optimization for quadratic unconstrained problems using a digital annealer. *Frontiers in Physics*, 7.
- Arute, F., et al. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779), 505–510.
- Arute, F., et al. (2020). Quantum Approximate Optimization Of The Maxcut Problem On A Superconducting Qubit Processor. *Nature Physics*, 16, 1043–1048.
- Avižienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1), 11-33.
- Bapst, V., Foini, L., Krzakala, F., Zdeborová, L., & Mézard, M. (2013). The Quantum Adiabatic Algorithm Applied To Random Optimization Problems: A Quantitative Study. *Physical Review X*, 3, 041008.
- Barak, B., Chou, C.-N., Goldenberg, L., & Servedio, R. A. (2020). Certified Randomness From A Two-state System. *Nature Physics*, 16, 281–286.
- Bennett, C. H., & Divincenzo, D. P. (2000). Quantum Information And Computation. *Nature*, 406, 247-255.
- Bergholm, V., et al. (2018). Pennylane: Automatic differentiation of hybrid quantum-classical computations. *arXiv preprint arXiv:1811.04968*.
- Bernstein, D. J. & Lange, T. (2017). Post-quantum cryptography. *Nature*, 549(7671), 188–194.
- Biamonte, J. D. & Love, P. J. (2008). Realizable Hamiltonians For Universal Adiabatic Quantum Computation. *Physical Review A*, 78, 012352.
- Biamonte, J. D., Bergholm, V., & Whitfield, J. D. (2011). Adiabatic Quantum Simulation Of Quantum Field Theory In One Dimension. *Physical Review Letters*, 106, 150501.
- Biamonte, J., Bergholm, V., & Whitfield, J. D. (2008). Quantum Simulation Of Quantum Field Theory Using Continuous-variable Cluster States. *Physical Review A*, 78, 022303.

- Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S. (2017). Quantum machine learning. *Nature*, 549(7671), 195–202.
- Biswas, S. & Das, P. (2023). Analysis of quantum cryptology and the RSA algorithms defense against attacks using shor's algorithm in a post quantum environment. In *International Conference on Computational Intelligence in Communications and Business Analytics*, pp. 72–87, Springer.
- Boixo, S., et al. (2016). "characterizing Quantum Supremacy In Near-term Devices." *Nature Physics*, 12, 1031-1037.
- Boixo, S., et al. (2016). Computational Multiqubit Tunnelling In Programmable Quantum Annealers. *Nature Physics*, 12, 1038-1044.
- Boixo, S., Isakov, S. V., Zlokovic, M., & Royer, J. (2018). Characterizing Quantum Supremacy In Near-term Devices. *Nature Physics*, 14, 595-600.
- Breuer, H. P., & Petruccione, F. (2002). *The Theory Of Open Quantum Systems*. Oxford University Press.
- Browne, D. & Briegel, H. (2016). One-way quantum computation. In *Quantum information: From foundations to quantum technology applications*, pp. 449–473.
- Bukov, M., Day, A. R. R., Sels, D., Weinberg, P., Polkovnikov, A., & Mehta, P. (2018). Reinforcement Learning For Optimization Of Quantum Control Pulses. *Physical Review X*, 8, 031086.
- Cacciapuoti, A. S., Caleffi, M., Tafuri, F., Cataliotti, F. S., Gherardini, S., & Bianchi, G. (2019). Quantum internet: Networking challenges in distributed quantum computing. *IEEE Network*, 34(1), 137–143.
- Cerezo, M., et al. (2021). Variational quantum algorithms. *Nature Reviews Physics*, 3(9), 625–644.
- Chamberland, C., et al. (2020). Experimental Demonstration Of A Surface Code On A Superconducting Qubit Array. *Physical Review X*, 10, 041064.
- Childs, A. M., Farhi, E., Goldstone, J., & Gutmann, S. (2013). Robustness Of Adiabatic Quantum Computation. *Physical Review A*, 87, 022339.
- Clarke, J., & Wilhelm, F. K. (2008). Superconducting Quantum Bits. *Nature*, 453, 1031-1042.
- Córcoles, A. D., Kandala, A., Javadi-Abhari, A., McClure, D. T., Cross, A. W., Temme, K., Nation, P. D., Steffen, M., & Gambetta, J. M. (2019). Challenges and opportunities of near-term quantum computing systems. *Proceedings of the IEEE*, 108(8), 1338–1352.
- Cross, A. (2018). The ibm q experience and qiskit open-source quantum computing software. In *APS March meeting abstracts*, vol. 2018, pp. L58–003.
- Daley, A. J., Bloch, I., Kokail, C., Flannigan, S., Pearson, N., Troyer, M., & Zoller, P. (2022). Practical quantum advantage in quantum simulation. *Nature*, 607(7920), 667–676.

- De Leon, N. P., et al. (2021). Materials challenges and opportunities for quantum computing hardware. *Science*, 372(6539), eabb2823.
- De Stefano, M., Pecorelli, F., Di Nucci, D., Palomba, F., & De Lucia, A. (2022). Software engineering for quantum programming: How far are we? *Journal of Systems and Software*, 190, 111326.
- Devoret, M. H., & Schoelkopf, R. J. (2013). Superconducting Circuits For Quantum Information: An Outlook. *Science*, 339, 1169-1174.
- Dickson, N. G., Amin, M. H. S., Blanchard, L., Dumoulin, E., & Laforest, M. (2013). Thermally Assisted Quantum Annealing Of A 16-qubit Superconducting Circuit. *Nature Communications*, 4, 1-7.
- Dickson, N. G., Amin, M. H., & Bergeron, D. (2013). Thermally Assisted Quantum Annealing: A Correction To The Quantum Annealing Process. *Physical Review Letters*, 111, 100502.
- Ding, C., Bao, T.-Y., & Huang, H.-L. (2021). Quantum-inspired support vector machine. *IEEE Transactions on Neural Networks and Learning Systems*, 33(12), 7210–7222.
- DiVincenzo, D. P. (2000). The Physical Implementation Of Quantum Computation. *Fortschritte Der Physik*, 48(9-11), 771-783.
- Du, W., Li, B., & Tian, Y. (2008). Quantum annealing algorithms: State of the art. *Jisuanji Yanjiu yu Fazhan/Computer Research and Development*, 45(9), 1501-1508.
- Farhi, E., et al. (2015). Quantum Adiabatic Algorithms And Large Spin Tunneling. *Physical Review A*, 90, 032315.
- Farhi, E., Goldstone, J., & Gutmann, S. (2011). A Quantum Approximate Optimization Algorithm. *Arxiv Preprint Arxiv:1106.3765*.
- Farhi, E., Goldstone, J., & Gutmann, S. (2014). A quantum approximate optimization algorithm. *arXiv preprint arXiv:1411.4028*.
- Farhi, E., Goldstone, J., Gutmann, S., Lapan, J., Lundgren, A., & Preda, D. (2001). A Quantum Adiabatic Evolution Algorithm Applied To Random Instances Of An Np-complete Problem. *Science*, 292, 472-476.
- García, C. R., Rommel, S., Takarabt, S., Olmos, J. J. V., Guilley, S., Nguyen, P., & Monroy, I. T. (2024). Quantum-resistant transport layer security. *Computer Communications*, 213, 345–358.
- Gill, S. S. (2021). Quantum and blockchain based serverless edge computing: A vision, model, new trends and future directions. *Internet Technology Letters*, e275.
- Gill, S. S., et al. (2024). Modern computing: Vision and challenges. *Telematics and Informatics Reports*, 13, 1–38.
- Gill, S. S., et al. (2022). Ai for next generation computing: Emerging trends and future directions. *Internet of Things*, 19, 100514.

- Gill, S. S., Kumar, A., Singh, H., Singh, M., Kaur, K., Usman, M., & Buyya, R. (2022). Quantum computing: A taxonomy, systematic review and future directions. *Software: Practice and Experience*, 52(1), 66–114.
- Gottesman, D. (1996). “class Of Quantum Error-correcting Codes Saturating The Quantum Hamming Bound.” *Physical Review A*, 56, 3292-3304.
- Gottesman, D. (1996). Class Of Quantum Error-correcting Codes Saturating The Quantum Hamming Bound. *Physical Review A*, 54, 1862-1865.
- Gottesman, D. (1997). Stabilizer Codes And Quantum Error Correction. *Physical Review A*, 56, 322-327.
- Gottesman, D. (2009). Class Of Quantum Error-correcting Codes Saturating The Quantum Hamming Bound. *Physical Review A*, 80, 022308.
- Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 212-219.
- Harris, R., Johansson, J., Berkley, A. J., Johnson, M. W., Lanting, T. M., & Bunyk, P. (2010). Experimental Demonstration Of A Robust And Scalable Flux Qubit. *Physical Review B*, 81, 134504.
- Heim, B., Soeken, M., Marshall, S., Granade, C., Roetteler, M., Geller, A., Troyer, M., & Svore, K. (2020). Quantum programming languages. *Nature Reviews Physics*, 2(12), 709–722.
- Hendrickx, N., Lawrie, W., Petit, L., Sammak, A., Scappucci, G., & Veldhorst, M. (2020). A single-hole spin qubit. *Nature communications*, 11(1), 3478.
- Hey, T. (1999). Richard Feynman and computation. *Contemporary Physics*, 40(4), 257–265.
- Howard, J., Lidiak, A., Jameson, C., Basyildiz, B., Clark, K., Zhao, T., Bal, M., Long, J., Pappas, D. P., Singh, M., et al. (2023). Implementing two-qubit gates at the quantum speed limit. *Physical Review Research*, 5(4), 043194.
- Illiano, J., Caleffi, M., Manzalini, A., & Cacciapuoti, A. S. (2022). Quantum internet protocol stack: A comprehensive survey. *Computer Networks*, 213, 109092.
- Johnson, M. W., Amin, M. H. S., Gildert, S., Lanting, T., Hamzehei, F., & Bunyk, P. (2011). Quantum Annealing With Manufactured Spins. *Nature*, 473, 194-198.
- Jordan, S. P., et al. (2006). “error Correction For Gate-based Quantum Computing With Non-abelian Anyons.” *Quantum Information And Computation*, 6, 251-264.
- Jordan, S. P., Farhi, E., & Shor, P. W. (2006). Error-correcting Codes For Adiabatic Quantum Computation. *Physical Review A*, 74, 052322.
- Jordan, S. P., Lee, K. S., & Preskill, J. (2012). Quantum Algorithms For Quantum Field Theories. *Science*, 336, 1130-1133.
- Kadowaki, T., & Nishimori, H. (1998). Quantum Annealing In The Transverse Ising Model. *Physical Review E*, 58, 5355-5363.

- Kandala, A., Mezzacapo, A., Temme, K., Takita, M., Brink, M., Chow, J. M., & Gambetta, J. M. (2017). Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets. *nature*, 549(7671), 242–246.
- Katzgraber, H. G., Hamze, F., Munoz-bauza, H., & Hoskinson, E. (2015). Glassy Phase Of Optimal Annealing. *Physical Review X*, 5, 031026.
- Kimmel, S., Low, G. H., & Yoder, T. J. (2015). Robust Calibration Of A Universal Quantum Gate Set Via Robust Phase Estimation. *Physical Review X*, 5, 021031.
- Krenn, M., Landgraf, J., Foesel, T., & Marquardt, F. (2023). Artificial intelligence and machine learning for quantum technologies. *Physical Review A*, 107(1), 010101.
- Kumar, A., et al. (2022). Securing the future internet of things with post-quantum cryptography. *Security and Privacy*, 5(2), e200.
- Kumar, A., et al. (2022). *Quantum and Blockchain for Modern Computing Systems: Vision and Advancements*. Springer.
- Lanting, T., et al. (2014). Entanglement In A Quantum Annealer. *Physical Review X*, 4, 021041.
- Lloyd, S. (1996). Universal Quantum Simulators. *Science*, 273, 1073-1078.
- Magesan, E., Gambetta, J. M., & Emerson, J. (2012). Robustness Of Quantum Gates In The Presence Of Noise. *Physical Review A*, 85, 042311.
- Mafu, M. & Senekane, M. (2021). Design and implementation of efficient quantum support vector machine. In *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, pp. 1–4, IEEE.
- Mandrà, S., Zhu, Z., Wang, W., & Zeng, A. (2017). Exponentially Biased Ground-state Sampling Of Quantum Many-body Systems With Quantum Annealing. *Physical Review Letters*, 119, 100502.
- Martinis, J. M., et al. (2009). "rabi Oscillations In A Josephson-junction Qubit." *Physical Review Letters*, 102, 100502.
- Mcgeoch, C. C., & Wang, G. (2013). Experimental Evaluation Of An Adiabatic Quantum Algorithm For Finding The Ground State Of A Spin Glass. *Physical Review A*, 88, 062314.
- Mermin, N. D. (2007). *Quantum Computer Science: An Introduction*. Cambridge University Press.
- Mikkelsen, M., Berezovsky, J., Stoltz, N., Coldren, L., & Awschalom, D. (2007). Optically detected coherent spin dynamics of a single electron in a quantum dot. *Nature Physics*, 3(11), 770–773.
- Morita, S., & Nishino, M. (2008). Mathematical Foundation Of Quantum Annealing. *Journal Of The Physical Society Of Japan*, 77, 104001.
- Mott, A., et al. (2017). Machine Learning For Error Correction In Quantum Annealing. *Science Advances*, 3, E1701812.

- Nadj-Perge, S., Frolov, S., Bakkers, E., & Kouwenhoven, L. P. (2010). Spin–orbit qubit in a semiconductor nanowire. *Nature*, 468(7327), 1084–1087.
- Nayak, C., Simon, S. H., Stern, A., Freedman, M., & Sarma, S. D. (2008). Non-abelian Anyons And Topological Quantum Computation. *Reviews Of Modern Physics*, 80, 1083–1159.
- Neven, H., Denchev, V. S., Macready, W. G., & Drew-brook, M. (2009). Training A Large-scale Classifier With The Quantum Adiabatic Algorithm. *Arxiv Preprint Arxiv:0903.1931*.
- Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press.
- Otterbach, J. S., et al. (2017). Quantum Control And Error Correction With Machine Learning. *Physical Review X*, 7, 041006.
- Paler, A. & Devitt, S. J. (2015). An introduction into fault-tolerant quantum computing. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1–6.
- Pednault, E., Gunnels, J. A., Nannicini, G., Horesh, L., & Wisnieff, R. (2019). Leveraging secondary storage to simulate deep 54-qubit sycamore circuits. *arXiv preprint arXiv:1910.09534*.
- Pérez-Castillo, R., Serrano, M. A., & Piattini, M. (2021). Software modernization to embrace quantum technology. *Advances in Engineering Software*, 151, 102933.
- Peruzzo, A., McClean, J., Shadbolt, P., Yung, M.-H., Zhou, X.-Q., Love, P. J., Aspuru-Guzik, A., & O'brien, J. L. (2014). A variational eigenvalue solver on a photonic quantum processor. *Nature communications*, 5(1), 4213.
- Piattini, M., Serrano, M., Perez-Castillo, R., Petersen, G., & Hevia, J. L. (2021). Toward a quantum software engineering. *IT Professional*, 23(1), 62–66.
- Pirandola, S. & Braunstein, S. L. (2016). Physics: Unite to build a quantum internet. *Nature*, 532(7598), 169–171.
- Preskill, J. (1998). Reliable Quantum Computers. *Proceedings Of The Royal Society A*, 454, 385-410.
- Preskill, J. (2018). Quantum computing in the nisq era and beyond. *Quantum*, 2, 79.
- Preskill, J. (2023). Quantum computing 40 years later. In *Feynman Lectures on Computation*, pp. 193–244, CRC Press.
- Ray, P., Chakrabarti, B. K., & Chakraborti, A. (1989). Sherrington-kirkpatrick Model In A Transverse Field: Quantum Annealing Using Tunnelling Barriers. *Journal Of Physics A: Mathematical And General*, 22, L1085-L1090.
- Rebentrost, P., Mohseni, M., & Lloyd, S. (2014). Quantum support vector machine for big data classification. *Physical review letters*, 113(13), 130503.

- Reed, M. D., DiCarlo, L., Nigg, S. E., Sun, L., Frunzio, L., Girvin, S. M., & Schoelkopf, R. J. (2012). Realization of three-qubit quantum error correction with superconducting circuits. *Nature*, 482(7385), 382–385.
- Rønnow, T. F., et al. (2014). Defining And Detecting Quantum Speedup. *Science*, 345, 420-424.
- Rozenman, G. G., Kundu, N. K., Liu, R., Zhang, L., Maslennikov, A., Reches, Y., & Youm, H. Y. (2023). The quantum internet: A synergy of quantum information technologies and 6G networks. *IET Quantum Communication*, 4(4), 147–166.
- Santoro, G. E., Martonak, R., Tosatti, E., & Car, R. (2006). Optimization Using Quantum Mechanics: Quantum Annealing Through Adiabatic Evolution. *Science*, 312, 1467–1470.
- Santoro, G. E., Martoňák, R., Tosatti, E., & Car, R. (2006). Theory Of Quantum Annealing Of An Ising Spin Glass. *Science*, 312, 264-267.
- Sasaki, T., Yamamoto, Y., & Koashi, M. (2014). Practical quantum key distribution protocol without monitoring signal disturbance. *Nature*, 509(7501), 475–478.
- Schoelkopf, R. J., & Girvin, S. M. (2008). "wiring Up Superconducting Qubits." *Nature Physics*, 4, 724-727.
- Serrano, M. A., Cruz-Lemus, J. A., Perez-Castillo, R., & Piattini, M. (2022). Quantum software components and platforms: Overview and quality assessment. *ACM Computing Surveys*, 55(8), 1–31.
- Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal On Computing*, 26, 1484-1509.
- Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2), 303–332.
- Silva, V. (2023). Richard Feynman, demigod of physics, father of the quantum computer. In *Quantum Computing by Practice: Python Programming in the Cloud with Qiskit and IBM-Q*, pp. 49–85, Springer.
- Simon, D. R. (1997). On the power of quantum computation. *SIAM journal on computing*, 26(5), 1474–1483.
- Singh, A., Dev, K., Siljak, H., Joshi, H. D., & Magarini, M. (2021). Quantum internet—applications, functionalities, enabling technologies, challenges, and research directions. *IEEE Communications Surveys & Tutorials*, 23(4), 2218–2247.
- Singh, M., et al. (2022). Quantum artificial intelligence for the science of climate change. In *Artificial Intelligence, Machine Learning and Blockchain in Quantum Satellite, Drone and Network*, pp. 199–207, CRC Press.
- Singh, R., et al. (2023). Edge AI: a survey. *Internet of Things and Cyber-Physical Systems*, 3, 71–92.
- Sisodia, M. (2020). Comparison the performance of five-qubit IBM quantum computers in terms of bell states preparation. *Quantum Information Processing*, 19(8), 215.

- Subramanian, T., et al. (2022). *Artificial Intelligence, Machine Learning and Blockchain in Quantum Satellite, Drone and Network*. CRC Press.
- Venturelli, D., & Kais, S. (2018). A Quantum Algorithm For Machine Learning. *Journal Of Physics: Conference Series*, 1230, 012001.
- Venturelli, D., & Kais, S. (2019). Quantum Annealing Of A Quantum Glass. *Physical Review Letters*, 123, 140501.
- Venturelli, D., Do, R., Rieffel, E., & Frankel, S. (2018). Quantum Annealing Correction For Random Ising Problems. *Physical Review A*, 98, 032324.
- Venuti, L. C., Albash, T., Whaley, K. B., & Lidar, D. A. (2016). Adiabatic Quantum Simulation Of A Lattice Gauge Theory In One Dimension. *Physical Review X*, 6, 041021.
- Vietz, D., Barzen, J., Leymann, F., & Wild, K. (2021). On decision support for quantum application developers: categorization, comparison, and analysis of existing technologies. In *International Conference on Computational Science*, pp. 127–141, Springer.
- Viola, L., et al. (1999). "dynamical Decoupling Of Quantum Systems From Their Environment." *Physical Review Letters*, 82, 2417-2420.
- Viola, L., et al. (2019). Dynamical Decoupling Of A Superconducting Qubit Array From Unwanted Interactions With The Environment. *Nature Communications*, 10, 1-8.
- Vourdas, A. (2004). Quantum systems with finite Hilbert space. *Reports on Progress in Physics*, 67(3), 267.
- Walia, G. K., et al. (2023). AI-empowered fog/edge resource management for iot applications: A comprehensive review, research challenges and future perspectives. *IEEE Communications Surveys & Tutorials*.
- Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science*, 362(6412), eaam9288.
- Williams, C. P. (2011). *Quantum Gates*. London: Springer London.
- Willsch, M., et al. (2020). Support Vector Machines On The D-wave Quantum Annealer. *Quantum Machine Intelligence*, 2, 1–13.
- Yang, Z., Zolanvari, M., & Jain, R. (2023). A survey of important issues in quantum computing and communications. *IEEE Communications Surveys & Tutorials*.
- Zhou, L., Wang, H., & Li, M. (2020). Quantum Approximate Optimization Algorithm For The Maxcut Problem On A Random Graph. *Physical Review A*, 102, 022601.

5.2. Sources Web et Autres Documents

- Chatterjee, A., Phalak, K., & Ghosh, S. (n.d.). *Quantum Error Correction For Dummies*. arXiv.
- D-wave Systems Inc. (n.d.). *D-wave 2000Q Quantum Annealer*.
- D-wave Systems Inc. (n.d.). *D-wave Quantum Annealer Architecture*.

- IBM. (n.d.). *What is quantum computing?*. IBM.
- IBM Research. (n.d.). *Quantum Computing*.
- Quantum News. (2024, 31 août). *Quantum Annealing vs Gate-Based Quantum Computing. What's the Difference*. Quantum Zeitgeist.
- Reddit. (n.d.). *Explain it like I'm 5?*. r/QuantumComputing.
- Tepanyan, H. (n.d.). *What Is Quantum Computing and How Does It Work?*. BlueQubit.