

Synthèse de Veille

1- LE DOMAINE DE L'INFORMATIQUE QUANTIQUE

L'informatique quantique plonge ses racines dans la physique quantique, se distinguant ainsi de la physique classique en explorant les échelles infiniment petites, atomiques et subatomiques, ainsi que les lois physiques qui gouvernent ces mondes.

Dans le contexte de l'informatique quantique, deux comportements distincts sont exploités : la superposition et l'intrication.

La superposition quantique suggère qu'un système quantique, tel qu'une particule, peut occuper simultanément deux états, c'est-à-dire avoir plusieurs valeurs pour une certaine quantité observable. Par exemple, un électron peut présenter des spins (champs magnétiques) différents, positifs, négatifs, ou les deux en même temps.

Quant à l'intrication quantique (ou enchevêtrement quantique), il s'agit d'un phénomène impliquant deux particules ayant des états quantiques interdépendants. Cela signifie qu'un changement d'état de l'une de ces particules intriquées entraînera automatiquement un changement d'état de son homologue. Pour illustrer, prenons l'exemple de deux électrons créés dans un état intriqué : la mesure du spin négatif de l'un entraînera inévitablement un spin positif pour l'autre, indépendamment de la distance entre eux.

2- Par delà le binaire

L'informatique quantique révolutionne notre approche traditionnelle basée sur des bits (0 et 1). Grâce aux "Qubits" qui suivent les règles quantiques, notamment la superposition, ils peuvent représenter non seulement 0 ou 1, mais aussi les deux simultanément. Cette caractéristique promet une augmentation significative de la puissance de calcul des ordinateurs quantiques. Cependant, bien que ces machines se révèlent efficaces pour certaines tâches, comme la factorisation de nombres premiers, elles ne garantissent pas une accélération pour tous les types de calculs. De plus, la création d'algorithmes quantiques adaptés et la résolution de problèmes sans solution actuelle demeurent des défis à surmonter dans le domaine de l'informatique quantique.

3-Des Défis majeurs

Entre la décohérence quantique, qui complique la lecture des Qubits sans altération, et la nécessité de maintenir une température extrêmement basse avec des ordinateurs cryogéniques, la route vers un ordinateur quantique opérationnel sur

nos bureaux est semée d'obstacles. Ces défis, liés à la destruction de la superposition lors de la lecture et à la complexité de maintenir la stabilité des qubits, soulignent les nombreux aspects techniques à résoudre avant de voir une adoption généralisée de cette technologie.

4-Mais aussi des avancés

Les avancées dans le domaine de l'informatique quantique sont marquées par des réponses créatives aux défis techniques. Atos propose un émulateur quantique, le Quantum Learning Machine, pour aider à concevoir des algorithmes. IBM travaille sur un algorithme de détection d'erreurs avec des Qubits supraconducteurs, tandis que Microsoft explore les Qubits Topologiques pour une stabilité accrue. Depuis la première opération de calcul réussie en 2002, les progrès se multiplient, avec D-Wave lançant le premier ordinateur quantique commercialisable en 2011 et Intel présentant récemment une puce de 49 Qubits au CES, soulignant une avancée significative vers une informatique quantique commerciale.

Conclusion :

L'informatique quantique, bien que loin d'une réalisation opérationnelle, demeure un sujet majeur de recherche pour des acteurs clés tels que Microsoft, IBM, la NASA, et d'autres. L'objectif partagé est d'atteindre la suprématie quantique, dépassant les capacités des ordinateurs classiques. Les applications envisagées sont vastes, allant de la création de nouveaux matériaux à des avancées médicales révolutionnaires. Toutefois, ces avancées soulèvent des préoccupations, notamment en matière de cybersécurité, avec des initiatives telles que Risq qui travaillent sur des solutions de chiffrement post-quantique. Malgré ces opportunités passionnantes, des progrès substantiels et la résolution de défis technologiques et de sécurité restent nécessaires avant une adoption généralisée de l'informatique quantique.