Communiqués de presse

IBM dévoile 5 innovations qui changeront nos vies dans les 5 années à venir

ARMONK, N.Y. - 19 mars 2018: IBM (NYSE: IBM) annonce aujourd'hui ses prédictions annuelles « 5in5 », mettant en évidence les innovations scientifiques et technologiques qui, selon la compagnie, auront un impact majeur sur notre vie quotidienne au cours des cinq prochaines années. Les prédictions couvrent les domaines technologiques les plus évoqués actuellement, en particulier l'intelligence artificielle, l'informatique quantique, la blockchain et la cybersécurité.

- Nos océans sont pollués. Des microscopes robotisés alimentés par de l'intelligence artificielle peuvent les sauver.
- Personne n'aime les imitations. Les crypto-ancres et la blockchain s'uniront contre les faussaires.
- Les pirates vont pirater. Jusqu'à ce qu'ils rencontrent la cryptographie par réseau euclidien.
- Les biais relatifs à l'intelligence artificielle vont exploser. Mais seule l'IA impartiale survivra.
- Aujourd'hui, l'informatique quantique est le terrain de jeu des chercheurs. Dans cinq ans, elle sera accessible au grand public.

Vous trouverez le détail de chacune de ces prédictions ci-dessous :

Nos océans sont pollués. Des microscopes robotisés alimentés par de l'intelligence artificielle (IA) peuvent les sauver.

Dans cinq ans, de petits microscopes autonomes à base d'IA, mis en réseau dans le Cloud et déployés dans le monde entier, surveilleront en permanence l'état de la ressource naturelle la plus critique pour notre survie : l'eau.

D'ici 2025, plus de la moitié de la population mondiale vivra dans des zones soumises à un stress hydrique. Mais les scientifiques ont du mal à collecter et analyser en temps réel les données les plus élémentaires concernant les conditions de nos océans, lacs et rivières.

Il existe des détecteurs spécialisés qui peuvent être déployés pour détecter des produits chimiques et des conditions spécifiques dans l'eau, mais ils passent à côté de certains éléments imprévus, telles que les espèces invasives ou l'introduction de nouveaux composants chimiques provenant du ruissellement.

Le plancton, cependant, est un détecteur biologique naturel de la santé aquatique. Même de légères modifications de la qualité de l'eau affectent son comportement. Il constitue également la base de la chaîne

alimentaire océanique, qui représente la source principale de protéines pour plus d'un milliard de personnes. Pourtant, on sait très peu de choses sur la façon dont le plancton se comporte dans son habitat naturel, car son étude exige généralement de prélever des échantillons et de les expédier à un laboratoire.

Les chercheurs d'IBM conçoivent de petits microscopes autonomes qui peuvent être placés dans des plans d'eau afin de surveiller le plancton *in situ*, d'identifier différentes espèces et de suivre leur mouvement en trois dimensions. Ces résultats peuvent être utilisés pour mieux comprendre son comportement, tel que la façon dont il réagit aux changements dans son environnement causés par différents facteurs, de la température, aux marées noires, aux ruissellements. Ils pourraient même être utilisés pour prédire les menaces concernant notre approvisionnement en eau, telles que les marées rouges.

Ce microscope n'a pas de lentille et repose sur une puce d'imagerie, comme celle que l'on trouve dans n'importe quel téléphone cellulaire. Elle capture l'ombre du plancton pendant qu'il nage sur la puce, générant un échantillon numérique de sa santé, sans avoir besoin de focalisation.

À l'avenir, ce microscope pourrait être doté d'une technologie d'IA à haute performance et à faible puissance pour analyser et interpréter les données localement, pouvant signaler toute anomalie en temps réel afin de pouvoir agir immédiatement.

Parce que ce qui est bon pour le plancton est bon pour nous tous.

Remerciements : Ce matériel est basé sur des travaux soutenus par la National Science Foundation sous la concession n° DBI-1548297. Les opinions, constatations et conclusions ou recommandations exprimées dans ce document sont celles de(s) auteur(s) et ne reflètent pas nécessairement les opinions de la National Science Foundation.

Personne n'aime les imitations. Les crypto-ancres et la blockchain s'uniront contre les faussaires.

Dans les cinq prochaines années, les ancres cryptographiques et la technologie blockchain garantiront l'authenticité d'un produit - depuis sa source jusqu'au client.

La fraude coûte à l'économie mondiale plus de 600 milliards de dollars par an. Et dans quelques pays, près de 70% de certains médicaments vitaux sont contrefaits.

Empêcher les acteurs malveillants de tout falsifier, de la monnaie papier à l'électronique grand public, devient difficile à cause de chaînes d'approvisionnement complexes - composées de dizaines de fournisseurs dans plusieurs pays.

Les ancres cryptographiques sont des empreintes numériques inviolables que les chercheurs d'IBM sont en train d'élaborer pour les intégrer dans des produits ou des parties de produits et les lier à la blockchain. Ces empreintes digitales peuvent prendre de nombreuses formes, mais lorsqu'elles sont liées à une blockchain, elles représentent un puissant moyen de prouver l'authenticité d'un produit.

Par exemple, un dispositif de test sanguin en plastique pour le dépistage du paludisme - qui est contrefait par millions et qui est présenté comme authentique en Afrique - pourrait être gravé avec un code optique inaltérable. Même les pilules individuelles contre le paludisme peuvent être enduites d'une teinte d'encre magnétique comestible. Par le simple scan d'un smartphone, un médecin ou un patient peut immédiatement vérifier que son médicament est sûr et authentique.

Mais que se passe-t-il si vous essayez de garantir l'authenticité d'un contenu liquide, tel qu’une bouteille de Bordeaux de 1982, ou d’un métal coûteux et que vous ne pouvez pas insérer directement une ancre crypto sur l'objet ?

Les scientifiques d'IBM ont également couvert cela, avec une crypto-ancre disponible dès aujourd'hui. Cette approche combine un capteur mobile ou un téléphone portable équipé d'un dispositif optique spécial et des algorithmes d’intelligence artificielle pour apprendre et identifier la structure optique et chacune des caractéristiques à partir d'une étiquette en papier – et cela prend autant de temps que de faire un selfie. Il peut également identifier la présence de séquences d'ADN en quelques minutes.

Certaines crypto-ancres feront plus qu’authentifier des biens physiques. Le plus petit ordinateur au monde (littéralement) est une architecture de point d’accès conçue par IBM et une plateforme informatique qui est

plus petite qu'un grain de sel. Il coûtera moins de dix cents à fabriquer, et peut surveiller, analyser, communiquer et même agir sur des données. Il comprend plusieurs centaines de milliers de transistors sur une surface à peine visible à l'œil nu, et peut aider à vérifier qu'un produit a été manipulé correctement tout au long de son long parcours.

Ces crypto-ancres ouvrent la voie à de nouvelles solutions qui abordent la sécurité alimentaire, l'authenticité des composants manufacturés, les produits génétiquement modifiés, l'identification des objets contrefaits et la provenance des produits de luxe. Les premiers modèles pourraient être mis à la disposition des clients dans les 18 prochains mois. Au cours des cinq prochaines années, les progrès de la microfluidique, des plateformes d'emballage, de la cryptographie, de la mémoire non volatile et de la conception feront passer ces systèmes du laboratoire au marché.

Les pirates vont pirater. Jusqu'à ce qu'ils rencontrent la cryptographie par réseau euclidien.

L'ampleur et la sophistication des cyberattaques augmentent chaque année, tout comme les enjeux. Dans cinq ans, de nouvelles méthodes d'attaque rendront les mesures de sécurité actuelles terriblement inadéquates.

Par exemple, dans plusieurs années, un ordinateur quantique universel, tolérant aux pannes, avec des millions de qubits pourrait rapidement passer au crible les probabilités et décrypter même le chiffrement courant le plus puissant, rendant cette méthodologie de sécurité fondamentale obsolète.

Les chercheurs d'IBM développent une nouvelle méthode de sécurité conçue pour répondre à cette fatalité. Elle est conçue sur une architecture sous-jacente connue sous le nom de cryptographie par réseau euclidien, qui cache des données à l'intérieur de structures algébriques complexes appelées réseaux euclidiens.

Voici comment cela fonctionne. En mathématiques, les réseaux euclidiens présentent des problèmes qui sont considérés comme très difficiles à résoudre. L'un de ces problèmes est appelé problème du vecteur le plus court : trouver le point dans le réseau le plus proche de l'origine. La difficulté à résoudre ces problèmes est utile pour les cryptographes, car ils peuvent appliquer cette insolubilité pour protéger les informations, même lorsque les ordinateurs quantiques sont assez forts pour craquer les techniques de chiffrement actuelles.

La cryptographie basée sur un réseau euclidien n'est pas seulement destinée à contrecarrer les futurs ordinateurs quantiques. Ce couteau suisse d’algèbre cryptographique est également à la base d'une autre technologie de chiffrement homomorphe appelée FHE (Fully Homomorphic Encryption).

Aujourd'hui, les fichiers sont chiffrés en transit et au repos, mais déchiffrés en cours d'utilisation. Ce processus permet aux pirates de visualiser ou de voler des fichiers non chiffrés.

Les technologies cryptographiques de calcul sécurisé, telles que le FHE, éliminent cette vulnérabilité en permettant le calcul sur les données par différents utilisateurs même si le fichier reste chiffré.

Jusqu'à récemment, le FHE était trop lent et coûteux pour être utilisé largement. Mais les techniques d'optimisation algorithmique et d'accélération matérielle ont réduit le temps et les coûts d'utilisation du FHE de plusieurs ordres de grandeur. Les calculs qui auraient requis des années peuvent désormais être effectués en quelques heures ou même minutes.

Le FHE et d'autres outils de calcul sécurisé pourraient permettre à plusieurs entités coopérantes d'effectuer des calculs sur un fichier sans jamais voir des données sensibles ou les exposer à des pirates informatiques.

Par exemple, une agence d'évaluation du crédit à la consommation pourrait analyser et produire des scores de crédit sans jamais déchiffrer les données personnelles. De plus, les médecins traitants pourraient partager les dossiers médicaux des patients avec des spécialistes, des laboratoires, des chercheurs en génomique et des entreprises pharmaceutiques de manière à permettre à chaque partie d'accéder aux données pertinentes sans jamais révéler l'identité du patient.

La bonne nouvelle est que la communauté de la sécurité prépare déjà l'avenir. En fait, en décembre dernier, les scientifiques d'IBM ont soumis leurs techniques de chiffrement post-quantique à l'Institut National des Normes et de la Technologie pour qu'ils les considèrent comme une norme mondiale ; un pas de plus vers la fin de la course aux armements pour la cybersécurité.

Les biais relatifs à l’intelligence artificielle (IA) vont exploser. Mais seule l'IA impartiale survivra.

Dans cinq ans, le nombre de systèmes et d'algorithmes d'IA biaisés augmentera, tout comme cela a été le cas des virus informatiques au tout début. Mais nous traiterons ces dérives avec une approche similaire, à la fois en fournissant des solutions pour maîtriser les biais dans l'intelligence artificielle et en promouvant des

systèmes d'intelligence artificielle sans ces biais.

Les systèmes d'IA sont simplement aussi bons que les données avec lesquelles nous les alimentons. Les mauvaises données peuvent contenir des préjugés raciaux, sexistes ou idéologiques implicites. De nombreux systèmes d'IA continueront d'être formés en utilisant de mauvaises données, ce qui constitue un problème permanent. Mais nous pensons que les biais peuvent être maîtrisés et que les systèmes d'IA qui s'y attaqueront auront le plus grand succès.

Alors que les humains et l'intelligence artificielle travaillent de plus en plus ensemble pour prendre des décisions, les chercheurs investiguent des moyens de s'assurer que le biais humain n'affecte pas les données ou les algorithmes utilisés pour éclairer ces décisions.

Les efforts du MIT-IBM Watson AI Lab sur la prospérité partagée s'inspirent des progrès récents de l'intelligence artificielle et de la modélisation cognitive computationnelle. Les approches contractuelles en matière d’éthique, pour décrire les principes que les personnes utilisent dans la prise de décision et déterminer comment les esprits humains les appliquent, vont dans ce sens. L'objectif est de concevoir des machines qui appliquent certaines valeurs et principes humains dans la prise de décision.

Un principe crucial, tant pour les humains que pour les machines, est d'éviter les préjugés et donc d'empêcher la discrimination. Le biais dans un système d’IA se produit principalement dans les données ou dans le modèle algorithmique. Alors que nous travaillons à développer des systèmes d’IA auxquels nous pouvons faire confiance, il est essentiel de développer et de former ces systèmes avec des données non biaisées et de développer des algorithmes qui peuvent être facilement expliqués.

Dans ce but, les chercheurs d'IBM ont développé une méthodologie pour réduire les biais qui peuvent être présents dans un ensemble de données d'apprentissage, de sorte que tout algorithme d'IA qui apprendra de cet ensemble de données perpétuera le moins d'iniquité possible.

Les scientifiques d'IBM ont également mis au point une méthodologie pour tester les systèmes d'IA, même lorsque les données d'entraînement ne sont pas disponibles. Cette recherche propose qu'un système indépendant d'évaluation du biais puisse déterminer l'équité d'un système d’IA. Par exemple, le service d'IA pourrait être impartial et capable de compenser le biais de données (scénario idéal), ou il pourrait juste adopter les propriétés de biaisement apportées par son apprentissage (qui pourrait être résolu par des

techniques de débiaisement des données), ou il pourrait même introduire un biais que les données soient impartiales ou non (le pire scénario). L'utilisateur final de l'IA sera en mesure de déterminer la fiabilité de chaque système, en fonction de son niveau de partialité.

Identifier et atténuer les biais dans les systèmes d'IA est essentiel pour établir la confiance entre les humains et les machines qui apprennent. Au fur et à mesure que les systèmes d'IA décèlent, comprennent et soulignent les incohérences humaines dans la prise de décision, ils peuvent également révéler des manières dont nous sommes partiaux, sectaires et biaisés sur le plan cognitif, ce qui nous amène à adopter des points de vue plus impartiaux ou égalitaires.

Dans le processus de reconnaissance de nos préjugés et d’apprentissage aux machines de nos valeurs communes, nous pouvons améliorer plus que l'intelligence artificielle. Nous pouvons simplement nous améliorer.

Aujourd'hui, l'informatique quantique est le terrain de jeu des chercheurs. Dans cinq ans, elle sera accessible au grand public.

Dans cinq ans, les effets de l'informatique quantique dépasseront le laboratoire de recherche. L'informatique quantique ne sera plus cantonnée à la communauté scientifique, mais sera largement utilisée par de nouvelles catégories de professionnels et de développeurs qui se tournent vers cette nouvelle méthode de calcul pour résoudre des problèmes autrefois considérés comme insolubles.

Le quantique sera omniprésent dans les salles de cours des universités et sera même disponible, dans une certaine mesure, au lycée. Des cours d'informatique aux cours de chimie et de commerce, les étudiants se familiariseront avec cette technologie et poursuivront des carrières intégrant l'informatique quantique. Cette dernière sera profondément incorporée dans une gamme de programmes d'études, et son apprentissage sera un prérequis pour les programmes de sciences et d'ingénierie dans le monde entier. Aucun étudiant ne sera diplômé sans avoir été exposé à un enseignement consacré au quantique. Chaque université à l'échelle mondiale aura un programme d'informatique quantique et l’enseignera à ses étudiants à travers des expériences réelles et pratiques, fonctionnant sur des ordinateurs quantiques fonctionnels, accessibles via le Cloud.

Une nouvelle communauté de développeurs va émerger. Le concept d '« apprendre à coder » disposera d’une

filière quantique au sein du curriculum de l’informatique. Les algorithmes quantiques seront enseignés parallèlement aux algorithmes classiques en théorie de l'information.

Cette explosion de connaissances grand public contribuera, au cours des cinq prochaines années, à initier l'aube de l'ère quantique commerciale - une période de formation lors de laquelle la technologie de l'informatique quantique et ses cas d'usages précoces se développeront rapidement. Ces derniers utiliseront potentiellement des ordinateurs quantiques pour simuler précisément des molécules et des réactions chimiques de plus en plus grandes. Cela pourrait accélérer la recherche et, à l'avenir, conduire à la création de nouveaux matériaux, au développement de médicaments plus personnalisés ou à la découverte de sources d'énergie plus efficaces et durables.

Les chercheurs d'IBM ont déjà atteint des jalons importants en chimie quantique, ayant récemment utilisé un ordinateur quantique pour simuler avec succès la liaison atomique dans l'hydrure de béryllium (BeH2) ; la molécule la plus complexe jamais simulée par un ordinateur quantique. À l'avenir, les ordinateurs quantiques continueront de s'attaquer à des problèmes de plus en plus complexes, pour finalement rattraper et surpasser ce que nous pouvons faire avec les seules machines classiques.

Dans cinq ans, l'industrie aura découvert les premières applications pour lesquelles un ordinateur quantique (utilisé aux côtés d’un ordinateur classique) offrira un avantage dans la résolution de problèmes spécifiques. Les adopteurs précoces de l’ère de l’informatique quantique seront gratifiés d’un avantage certain.

À l'avenir, les ordinateurs quantiques ne seront plus considérés comme mystérieux. Le grand public va embrasser cette nouvelle ère, car notre compréhension collective de l'informatique quantique continuera à croître et à toucher chaque industrie et chaque établissement d'enseignement. Les concepts et le vocabulaire associés à l'informatique quantique ne seront plus vagues ou incompris, mais feront plutôt partie du vocabulaire courant. Les conversations autour de l'informatique quantique seront normales. Tout le monde saura ce qu'est un qubit - ou sera familiarisé avec l'idée.

Contact(s) relations externes

IBM

Gaëlle Dussutour Tél. : + 33 (0)1 58 75 17 96DUSGA@fr.ibm.com

Text100 pour IBM

Amélie Chipaux Tél. : + 33 (0) 6 62 49 20 50amelie.chipaux@text100.fr