Intelligence artificielle et chaînes de blocs : vulnérables aux cyberattaques

6 avril 2018

Auteur

Eric Lavallée

Associé, Agent de marques de commerce Associé, et Avocat

Les technologies qui reposent sur les chaînes de blocs (*blockchain* en anglais) et l'intelligence artificielle représentent un changement important pour notre société. La sécurité des données qui y sont échangées étant cruciale, l'adoption de ces solutions doit être planifiée dès aujourd'hui dans une optique à long terme.

Les entreprises sont nombreuses à mettre au point des services qui reposent sur les chaines de blocs, notamment dans le secteur des services financiers. Les cryptomonnaies, un exemple d'utilisation des chaînes de blocs, changent la manière dont s'effectuent certains échanges monétaires, loin du contrôle des institutions bancaires et des gouvernements.

Du côté de l'intelligence artificielle, les entreprises choisissent parfois des plateformes technologiques qui mettent en cause un partage des données dans le but d'accélérer la mise au point de leur outil d'intelligence artificielle.

L'impact de la révolution quantique sur la cybersécurité

En 2016, IBM a rendu accessible aux chercheurs un ordinateur permettant d'effectuer des essais sur divers algorithmes quantiques[1]. Il faut savoir que mode de fonctionnement des ordinateurs quantiques est radicalement différent de celui des ordinateurs conventionnels. D'ici une dizaine d'années, ils permettront d'effectuer rapidement des calculs qui dépassent la capacité des ordinateurs actuels les plus puissants. En effet, les ordinateurs quantiques utilisent les propriétés quantiques de la matière, notamment la superposition d'états, qui permet de traiter simultanément des ensembles de données liées.

L'algorithme de Shor est un algorithme utilisant des propriétés quantiques de la matière et qui peut être utilisé par des ordinateurs quantiques.

L'algorithme de Shor permet à un ordinateur quantique de factoriser un nombre entier très

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

rapidement, beaucoup plus que n'importe quel ordinateur conventionnel. Cette opération mathématique est l'élément essentiel permettant de déchiffrer l'information qui a été encryptée par plusieurs méthodes répandues en informatique. Cette technologie, qui intéresse les physiciens depuis longtemps, représente désormais un risque important pour la sécurité des données encryptées. Les données que l'on souhaite garder sécurisées et confidentielles présentent ainsi une vulnérabilité aux détournements à des fins non-autorisées.

Méthodes d'encryptages de chaînes de blocs : assez sécurisées?

Plusieurs méthodes d'encryptages existent aujourd'hui et plusieurs d'entre elles devront être renforcées pour maintenir la sécurité des données. Et il ne s'agit là que de quelques exemples de vulnérabilités aux ordinateurs quantiques.

Méthodes SHA-2 et SHA-3

Le National Institute of Standards and Technology (NIST) des États-Unis a émis des recommandations quant à la sécurité de diverses méthodes d'encryptage[2]. Les méthodes SHA-2 et SHA-3, qui sont les algorithmes qui servent à assurer l'intégrité des chaînes de blocs en produisant un « hachage » des blocs précédents, devront être renforcées pour maintenir le même niveau de sécurité.

Méthodes de signature utilisées par les Bitcoins et d'autres cryptomonnaies

> La cryptographie par courbes elliptique est un ensemble de techniques cryptographiques qui utilisent une ou plusieurs propriétés de fonctions mathématiques qui décrivent les courbes elliptiques afin d'encrypter des données.

Selon le NIST, la cryptographie par courbes elliptique deviendra inefficace. Ce qui est préoccupant, c'est qu'on parle ici de la méthode utilisée pour la signature de cryptomonnaies, dont le célèbre Bitcoin. Des recherches récentes indiquent que cette méthode présente une grande vulnérabilité à une attaque par des ordinateurs quantiques, qui pourraient déjouer ces codes en moins de dix minutes d'ici quelques années[3].

Algorithmes cryptographiques de type RSA

Les algorithmes cryptographiques de type RSA[4], très répandus pour la communication de données par Internet, sont particulièrement vulnérables aux ordinateurs quantiques. Ceci pourrait notamment avoir un impact si de grandes quantités de données devraient être échangées entre plusieurs ordinateurs, par exemple pour alimenter des systèmes d'intelligence artificielle.

Des algorithmes cryptographiques plus sécuritaires

Le NIST reconnait certaines approches qui sont plus sécuritaires. Un algorithme mis au point par Robert McEliece, mathématicien et professeur à Caltech, semble pouvoir résister à ces attaques[5] pour le moment. À plus long terme, on peut espérer que la technologie quantique permette elle-même de générer des clés sécuritaires.

Incidences juridiques et d'affaires en matière de protection des données

La loi impose aux entreprises l'obligation de protéger les renseignements personnels et confidentiels

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

qui leurs sont confiés par leurs clients. Elles doivent donc prendre des mesures adéquates pour protéger cet or brut que représentent les données.

Le choix d'une technologie d'intelligence artificielle ou de chaînes de blocs doit donc être effectué dès aujourd'hui, en tenant compte du fait qu'une fois adoptée, celle-ci sera utilisée pendant plusieurs années et sera possiblement appelée à survivre à l'arrivée des ordinateurs quantiques.

Qui plus est, il faudra également corriger les failles de sécurité des technologies n'étant pas sous le contrôle d'autorités gouvernementales ou d'une seule entreprise. Contrairement aux technologies plus conventionnelles, il ne s'agit pas d'installer une simple mise à jour sur un serveur unique. Dans certains cas, il faudra repenser la structure même d'une technologie décentralisée, telle la chaîne de blocs.

Faire le choix d'une technologie qui évolue

La clé sera donc de choisir une technologie qui permettra aux entreprises de respecter leurs obligations en matière de sécurité dans un monde post-quantique, ou à tout le moins de choisir une architecture qui permettra une modernisation de ces algorithmes d'encryptage en temps opportun. Il faudra donc établir un dialogue entre informaticiens, mathématiciens, physiciens et … avocats!

Lavery a mis sur pied le Laboratoire juridique Lavery sur l'intelligence artificielle (L3IA) qui analyse et suit les développements récents et anticipés dans le domaine de l'intelligence artificielle d'un point de vue juridique. Notre Laboratoire s'intéresse à tous les projets relatifs à l'intelligence artificielle (IA) et à leurs particularités juridiques, notamment quant aux diverses branches et applications de l'intelligence artificielle qui feront rapidement leur apparition dans toutes les entreprises et les industries.

---

1. Communiqué de presse : *IBM Makes Quantum Computing Available on IBM Cloud to Accelerate Innovation*: https://www-03.ibm.com/press/us/en/pressrelease/49661.wss; voir aussi : Linke, Norbert M., et al. "Experimental comparison of two quantum computing architectures." *Proceedings of the National Academy of Sciences* (2017): 201618020.
2. Chen, Lily, et al. *Report on post-quantum cryptography*. US Department of Commerce, National Institute of Standards and Technology, 2016.
3. Aggarwal, Divesh, et al. "Quantum attacks on Bitcoin, and how to protect against them." *arXiv preprint arXiv:1710.10377*(2017).
4. Il s'agit ici de l'acronyme des trois concepteurs de ce type d'encryptions, Rivest, Shamir et Adleman.
5. Supra, note 2; voir aussi Dinh, Hang, Cristopher Moore, and Alexander Russell. "McEliece and Niederreiter cryptosystems that resist quantum Fourier sampling attacks." *Annual Cryptology Conference*. Springer, Berlin, Heidelberg, 2011

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.