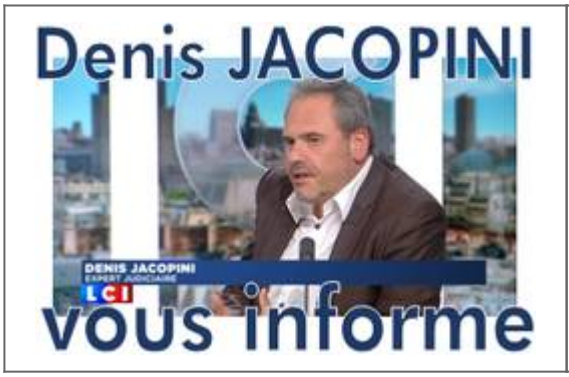
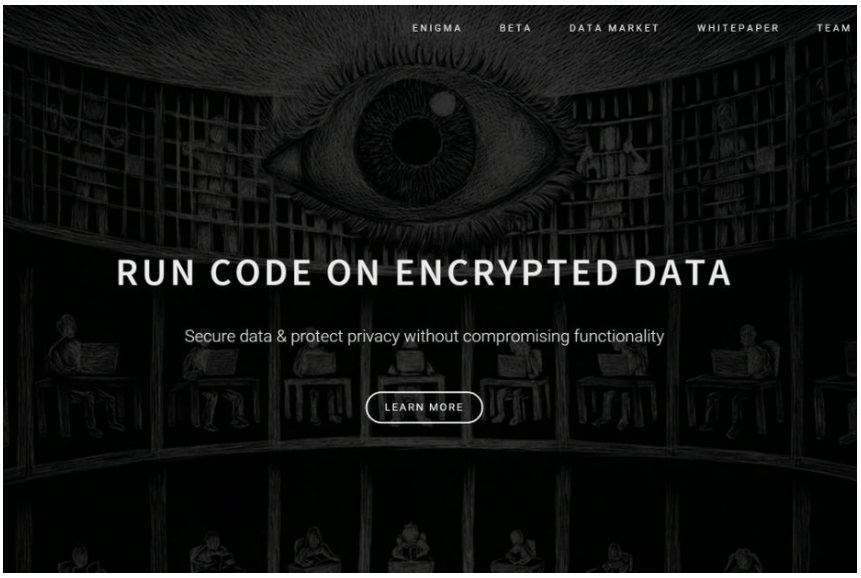
Enigma, le système de cryptage de données basé sur le blockchain du MIT Media Lab



Enigma, le système de cryptage de données basé sur le blockchain du MIT Media Lab

Avec Enigma, système de cryptage de données basé sur le blockchain, des informations confidentielles peuvent être stockées et partagées en ligne, sans intervention d'un tiers de confiance pour contrôler leur utilisation.



Enigma. Derrière ce nom mystérieux se cache l'une des dernières créations du MIT Media Lab, l'un des laboratoires de recherche du Massachusetts Institute of Technology. Ce système de cryptage de données est basé sur le blockchain, la technologie qui sous-tend le bitcoin (monnaie virtuelle mise en circulation en 2009). Elle fonctionne grâce au partage d'un registre d'informations par l'ensemble d'une communauté d'internautes.

Enigma, dont la version bêta sera lancée prochainement, permettra à des utilisateurs anonymes (particuliers, entreprises, associations…) de stocker dans le cloud et de partager des informations sensibles avec des tiers, de manière sécurisée. Pas besoin d'un intermédiaire de confiance, qui aurait accès à ces data pour contrôler leur utilisation et les crypter. Ces opérations sont effectuées par un réseau d'ordinateurs membres, grâce au système du blockchain. Les informations peuvent être traitées par des algorithmes, sans que le jeu de données brut ne soit jamais révélé dans sa totalité à l'une des parties.

DES RETOMBÉES DANS LE DOMAINE DU MACHINE LEARNING

Le registre blockchain, partagé par les ordinateurs membres du réseau, contrôle l'identité des utilisateurs d'Enigma (via un code, car ils sont anonymes) et leur donne accès ou non à tout ou partie des données. Il enregistre l'ensemble des opérations réalisées sur Enigma : enregistrement de nouvelles informations, consultation, opérations réalisées sur ces data…

Les données stockées par Enigma pourront être analysées par des applications et des logiciels extérieurs, tout en maintenant ces informations sous le contrôle de leur propriétaire. Le programme pourrait avoir des retombées intéressantes dans le domaine de la data science et du machine learning.

UN NOM DE BAPTÊME HISTORIQUE

Enigma pourrait également contribuer au développement d'un Internet des objets respectueux de la vie privée de ses utilisateurs, souligne le site spécialisé Bitcoin Magazine dans un article présentant le projet. Les propriétaires des données pourront, s'ils le souhaitent, les monétiser. Ils pourraient par exemple vendre à des laboratoires pharmaceutiques qui réalisent des recherches un accès partiel et contrôlé à leurs données de santé.

Guy Zyskind, étudiant au MIT, et Oz Nathan, entrepreneur qui a travaillé par le passé avec la défense israélienne, sont à l'origine de ce programme. Ils n'ont pas choisi son nom par hasard. Le système de cryptographie électro-mécanique utilisé par les Allemand pendant la deuxième guerre mondiale était baptisé Enigma. Un groupe de chercheurs, dont faisait notamment partie Alain Turing, a réussi à trouver la clef de ce code complexe.

Réagissez à cet article

Source : *Enigma, le système de cryptage de données basé sur le blockchain du MIT Media Lab*