RLDA 6612

Comprendre avant de juger : Explication du concept de Blockchain et étude de cas concrète

Pierre D'HUY
Ingénieur en Sécurité des Systèmes d'Information[1]

L'article 30 de la loi pour la confiance dans l'économie numérique dispose que :« *L'utilisation des moyens de cryptologie est libre* »[2].

Cet article reste cependant pondéré par de nombreuses réglementations et décrets secondaires agitant quelques fois le spectre du terrorisme ou de la criminalité pour légitimer ces restrictions. Au regard des circonstances récentes, le monde politique s'agite autour du sujet de la cryptographie et de la cryptologie sans en saisir nécessairement les tenants et les aboutissements et en blâmant sans cesse son utilisation par les criminels pour l'utilisation d'un internet « pédophile » ou de téléphones « incassables » par les services de renseignement. Mais il est nécessaire, pour le législateur et la justice, de s'émanciper de cette vision tronquée.

Cet article va d'abord chercher à démystifier les principes fondamentaux de la cryptologie puis à s'emparer de ces concepts pour les appliquer à la question de la blockchain ainsi qu'à son utilisation, légale ou illégale.

I. – Initiation aux concepts de la cryptologie

La cryptologie peut être définie comme le moyen de transformer un message en en garantissant la teneur et/ou le secret. Elle se compose de différents principes organisés autour de trois objectifs :

- Confidentialité : l'objectif est que les échanges ou les données stockées restent confidentielles. Cet objectif peut être réalisé tant à la fois par la distribution de données financières que par des flux d'informations protégées dans des pays sujets à une forte censure ;
- Authenticité : cet objectif permet de garantir l'origine d'une donnée et garantir de ce fait sa non-répudiation. Il peut permettre d'assurer des contraintes légales comme par exemple la signature d'un contrat ou le dépôt d'un appel d'offre à un marché publique ;
- Intégrité : cet objectif permet de s'assurer qu'un message soit resté constant et qu'il n'ait pas été modifié avant sa réception. De cet objectif découle la réalisation naturelle d'un objectif de traçabilité.

Ces objectifs reposent sur des propriétés mathématiques fortes permettant de démontrer un niveau de sécurité pour l'évaluation de la protection. Ces niveaux de sécurité ont été normalisés par des agences nationales comme l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ou son homologue américain, le National Institute of Standards and Technology (NIST).

Pour renforcer ces objectifs, la cryptologie utilise trois fonctions clefs : le chiffrement symétrique, le chiffrement asymétrique et les fonctions de condensats. D'autres fonctions existent également sur lesquelles reposent les précédentes ou permettant d'en élargir les objectifs.

Le chiffrement symétrique. Il consiste à utiliser une même clef servant pour chiffrer et déchiffrer les échanges. C'est le cas par exemple pour le chiffrement d'un document ou d'un ordinateur. La personne déchiffrant un message doit posséder le mot de passe ayant permis de le chiffrer. Ce principe de clef commune rend difficile les communications chiffrées avec un in-

(1) pierre.dhuy.net

(2) L. n° 2004-575, 21 juin 2004, pour la confiance dans l'économie numérique ; Article 30 : « *Utilisation, fourniture, transfert, importation et exportation de moyens de cryptologie* ».