La cybersécurité des documents numériques :

un cas d'usage concret de la blockchain

THIERRY ARNALY,

Président de
Autenthic Blockchain.

La cybersécurité est un sujet de plus en plus prégnant, non seulement à cause des tensions internationales et de l'action des mafias, mais surtout parce que notre vie, professionnelle et privée, est de plus en plus digitalisée.

Le confinement de 2020 a été un formidable accélérateur de cette virtualisation. Il était soudain devenu impossible de sortir de chez soi, de rencontrer d'autres personnes. Instantanément les échanges se sont fait par mail, visioconférence, appels téléphoniques, … Et tout de suite les ennuis ont commencé car une grande partie de la population n'était pas prête.

Cette accélération brutale de la digitalisation a été l'origine d'une hausse exponentielle de la fraude des documents échangés avec les professionnels du Droit et du Chiffre, au premier rang desquels on a trouvé les responsables juridiques et financiers des entreprises. La fraude la plus connue est celle des RIB, qui consiste à remplacer lors d'échanges par mail un RIB original par celui des pirates.

Un risque de préjudices élevés et multiples

Les professionnels sont de plus en plus nombreux à subir des préjudices à cause de ces falsifications. Il s'agit bien sûr immédiatement de pertes financières. Elles peuvent s'élever à plusieurs centaines de milliers d'euros et au-delà. Pour le moment, les assurances professionnelles semblent encore couvrir le risque, mais nul doute qu'elles modifieront leurs conditions pour ne pas se mettre en danger face à un risque répété.

Au-delà de l'aspect financier, les entreprises sont soumises à un risque sur leur image. En effet, se faire piéger en impliquant involontairement des clients ou des fournisseurs va laisser des traces et ternir l'image professionnelle de la société. Des brèches apparaîtront concernant sa capacité de gérer son système d'informations.

Pour terminer, à plus long terme, on peut se demander si des clients ou des fournisseurs victimes de l'incapacité de l'entreprise à se protéger de la falsification de ses documents numériques ne pourront pas se retourner contre elle et engager une action en justice en soulignant sa responsabilité et en demandant des dommages et intérêts.

La blockchain, une technologie de rupture facteur de confiance

Comment empêcher définitivement ces falsifications ? Il faut créer une référence pour chaque document créé ou transféré pour pouvoir s'assurer que le document qu'on a entre les mains est bien conforme à cette référence, à l'original.

On pourrait imaginer un organisme

central qui réaliserait cette tâche. Il devrait être interprofessionnel et international. De plus, il doit être complètement indépendant et transparent pour que personne ne puisse douter des références créées.

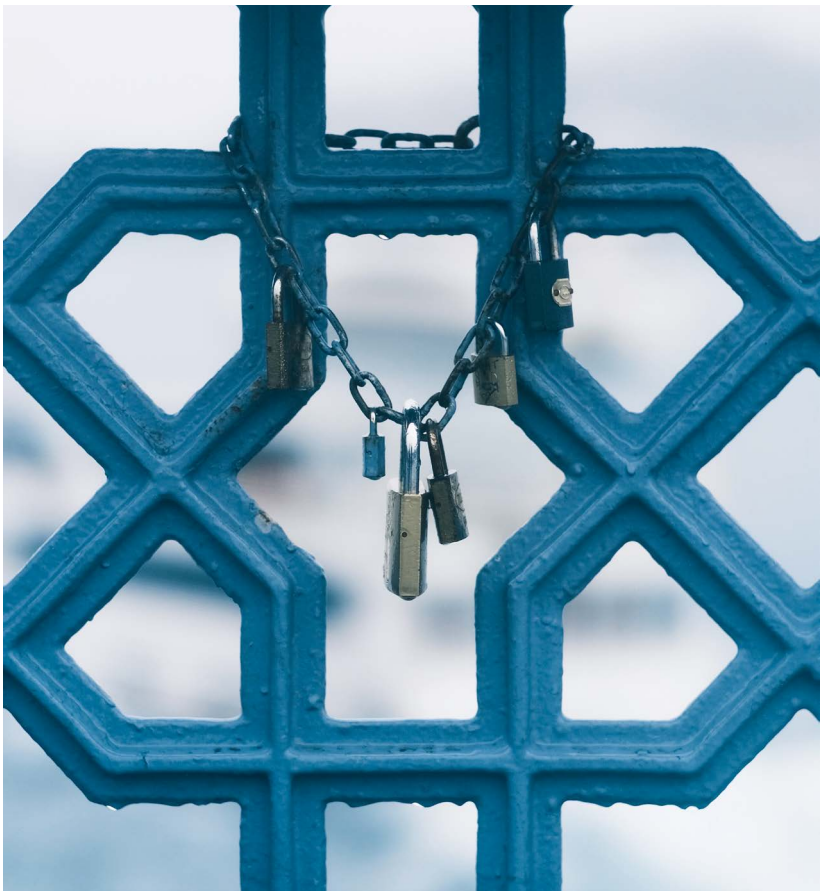
Aujourd'hui cet organisme n'existe pas, mais une technologie informatique révolutionnaire fournit ce service : la blockchain.

Cette technologie existe depuis une quinzaine d'années et son usage se diffuse lentement, mais surement, dans nos sociétés. Elle est connue en particulier pour servir de fondement au Bitcoin et autres cryptomonnaies. Elle est de plus en plus utilisée dans différents secteurs, de l'agriculture jusqu'au spatial, pour la confiance qu'elle confère aux informations qu'on y inscrit. En effet, elle n'autorise ni leur modification, ni leur suppression et elle leur attribue un horodatage certain, véritable preuve d'antériorité.

La blockchain fonctionne comme un registre qui serait dupliqué en temps réel sur des milliers de serveurs dans le monde et dont chaque page contient une référence infalsifiable, grâce à des algorithmes cryptographiques, qui synthétise le contenu des pages précédentes. De sorte que la moindre modification sur une page du registre sur un des serveurs est immédiatement détectée et corrigée.

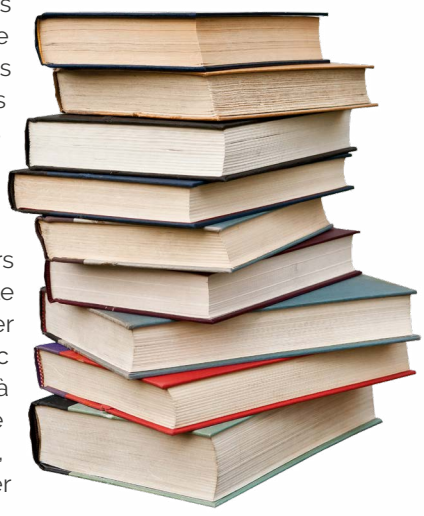
Authentic BlockChain utilise cette technologie pour garantir aux professionnels du Droit et du Chiffre que les documents numériques qu'ils sont amenés à traiter n'ont pas été falsifiés. La difficulté, outre le maniement de la blockchain elle-même, consiste à rendre la technologie invisible et à ne conserver que ses avantages.

Concrètement la sécurisation se passe de deux manières. Premier cas, lorsque le professionnel veut « figer » un document qu'il a créé, une première étape va consister à calculer l'empreinte numérique de ce fichier (Hash) avec une fonction comme SHA256 (qui se trouve sur tous les ordinateurs depuis des décennies). Cette empreinte (une suite de 32 caractères) est unique et ne permet pas de reconstituer



le fichier correspondant. C'est elle que l'on va écrire dans la blockchain. Authentic BlockChain utilise pour cela Polygon (MATIC), une blockchain publique de la famille Ethereum, ce qui permettra à terme de proposer de nouvelles fonctionnalités autour des smart contrats, qui sont des programmes informatiques exécutables inscrits dans la blockchain.

Conformément au RGPD, aucune information personnelle n'est inscrite dans la blockchain, puisqu'on ne pourrait plus les modifier ou les supprimer, même si la personne concernée le demandait. Toutes les informations personnelles sont donc remplacées par des codes dont on conserve les correspondances par ailleurs.



Le professionnel peut alors envoyer son fichier par mail. Le destinataire n'aura qu'à calculer son empreinte numérique avec la même fonction de hash et à la comparer avec celle stockée en blockchain. Si c'est la même, tout va bien ; sinon le fichier

a été modifié, par erreur ou pour une falsification.

Deuxième cas de sécurisation nécessaire, le professionnel veut récupérer un document en étant sûr qu'il n'a subi aucune modification. Il renseigne les coordonnées de son interlocuteur, celui-ci reçoit alors un mail lui indiquant la demande et lui permettant d'enclencher le processus, il arrive sur une page sécurisée où il saisit un code reçu par SMS pour s'identifier plus fortement, il sélectionne sur son ordinateur le fichier à transférer, celui-ci transite via une connexion sécurisée, son empreinte numérique est calculée et déposée dans la blockchain. Lorsque le professionnel veut le récupérer, avant de lui restituer revêtu d'un filigrane indiquant comment s'assurer de sa conformité avec l'original, le service contrôle que son empreinte numérique correspond toujours à celle déposée dans la blockchain. De cette manière, le document reçu est garanti à 100% conforme au document envoyé.

Un besoin de soutien en attendant l'adoption générale

La blockchain est encore considérée comme une technologie émergente et son adoption généralisée n'est pas prévue avant 2025. Pour le moment seuls quelques précurseurs utilisent cette technologie pour se mettre à l'abri de la fraude. Une « évangélisation » des entreprises et personnes concernées doit être réalisée (d'où cet article). La conduite du changement est fondamentale pour assurer une transition réussie. Un événement inattendu comme la pandémie pourrait accélérer ce processus, mais il vaut mieux ne pas le souhaiter.

L'usage de la technologie blockchain pour la cybersécurité des fichiers se différencie des coffres forts numériques et des signatures électroniques. Par rapport aux premiers, elle assure la sécurité même si le document n'est plus dans le coffre et elle permet de s'assurer de la conformité avec un fichier sans avoir à le divulguer. Par rapport aux secondes, elle ne nécessite pas de faire confiance à un acteur centralisé, elle conserve des informations opposables aux tribunaux (tel que l'horodatage) et elle fonctionne plus rapidement et à moindre coût.

Au final, ce qui est important, c'est de savoir que l'outil pour faire face à la falsification des documents numériques existe et qu'il faut se préparer à l'utiliser. La falsification des RIB n'est qu'une première étape et le risque de perte totale de confiance dans les informations échangées de façon numérique pourrait complètement bloquer les échanges et obliger à revenir à des remise de documents papier par des personnes formellement identifiées.

Le sens de l'histoire est bien sûr plutôt d'utiliser les bons outils, comme il y a une trentaine d'années lorsque tout le monde a commencé à se doter d'antivirus. Nul doute que, dans quelques années, la blockchain sera devenue une brique de cybersécurité évidente pour toutes les entreprises. ■