Association Nationale des Directeurs des Systèmes d'Information
www.andsi.fr

Blockchain

Compte rendu de la présentation du 13 décembre 2018, à la Terrasse

Compte rendu rédigé par Laure MUSELLI & ANDSI

En bref…

La blockchain, technologie sur laquelle reposent les crypto-monnaies et le bitcoin, devient aujourd'hui un sujet d'intérêt pour les entreprises, qui envisagent des cas d'usage liés à la possibilité qu'elle offre de se passer des tiers de confiance. Après avoir présenté les principes techniques du fonctionnement d'une blockchain, alliance de peer-to-peer et de cryptographie, Benjamin RAMEIX, DSI de Prévoir, revient sur l'histoire du bitcoin et les différents types de blockchain existants. Pierre BERLIOZ, professeur de droit, développe ensuite les enjeux juridiques liés à cette innovation, et notamment la question du cadre réglementaire à lui appliquer.

Benjamin RAMEIX, DSI de Prévoir : Principes et usages de la blockchain

La blockchain est souvent présentée comme une nouvelle technologie, alors qu'il s'agit plutôt d'un assemblage de technologies existantes : le peer-to-peer et la cryptographie. C'est en réalité l'approche proposée qui est nouvelle, en reposant sur un principe attrayant : se passer du tiers de confiance. Au-delà du bitcoin, entre attentes démesurées et rejet, la blockchain est un sujet émergent dans les entreprises, qui commencent à envisager et développer des cas d'usage.

Les principes d'une blockchain

Une blockchain se définit comme un **registre distribué**, c'est-à-dire un grand livre qui retrace un ensemble de transactions pouvant être de toute nature, allant des données d'un capteur de température à des bases notariales.

Il s'agit techniquement d'une **base de données** :

- **Distribuée** : le registre est déployé sur un ensemble d'ordinateurs, dans une logique de pair à pair.
- **Qui s'incrémente par bloc de transactions, de façon infalsifiable et transparente, grâce à des techniques de cryptographie.**

En ce sens, le registre ne constitue pas une base de données au sens SGDB ou SQL, comportant des téra-octets de données. Le bitcoin, de sa création à aujourd'hui, doit atteindre un maximum de 4 giga-octets.

Dans un système centralisé, un tiers de confiance, qui peut être un organe de l'État, tient à jour le registre, que chacun peut consulter ou incrémenter en passant par ce tiers de confiance.

Dans un système distribué tel que celui de la blockchain, le registre est ventilé sur l'ensemble des parties prenantes, et la confiance repose sur des **consensus de validation des transactions entre les nœuds du réseau,** établis dans le cadre d'un protocole de blockchain. Ces protocoles sont des règles qui visent à permettre la synchronisation du registre, tant sur l'intégrité de son état actuel que sur les nouvelles transactions soumises, en définissant lesquels des ordinateurs possédant une copie du registre font foi.

Il existe différents protocoles possibles, mais les deux principaux sont :

- **Le Proof of Work (PoW) :** selon cette logique, c'est la preuve de travail qui fait foi pour mettre à jour le registre, c'est-à-dire l'effort consenti par un nœud du réseau pour valider le bloc, à travers ce que l'on appelle le minage. On considère donc que dépenser beaucoup de CPU pour miner constitue une preuve de confiance. C'est sur ce consensus que repose le bitcoin. La logique de preuve de travail implique des consommations énergétiques assez énormes, de l'ordre de 40 térawatts par an de bitcoin, ce qui ramène le minage de bitcoins sur un an à la consommation énergétique de l'Etat d'Israël, c'est-à-dire 4 à 5 réacteurs nucléaires.
- **Le Proof of Stake (PoS) :** selon ce consensus, c'est la preuve d'enjeu qui fait foi. Autrement dit, on considère qu'un nœud du réseau qui a déjà en son sein un plus grand nombre de transactions, de crypto-données, que les autres, est digne de confiance.

L'histoire de la cryptographie remonte à l'antiquité :

Le **chiffre mono-alphabétique** est basé sur une substitution d'une lettre par une autre.

Le **chiffrement de César** repose sur une logique de chiffrement mono-alphabétique et une permutation circulaire de l'alphabet de rang 3. Sa limite tient à la possibilité d'observer la fréquence des lettres (le « E » par exemple) pour déchiffrer le code en fonction de la langue utilisée.

Le **chiffre de Vigenère** apporte une touche de modernité en découpant le message à chiffrer en blocs de longueurs égales et en appliquant une clé de permutation de k nombres de 0 à 25 sur chaque lettre. Deux lettres identiques pourront donc être chiffrées de manières différentes, ce qui augmente la sécurité.

Dans le cas de la **machine Enigma**, la clé correspond au choix de 3 disques, à la position initiale des disques et au couplage de 20 lettres.

Vernam et Mauborgne démontrent que pour un système de chiffrement totalement inviolable, la clé doit être générée de façon aléatoire, être aussi longue que le message, et être détruite immédiatement après. Ce système parfait est inapplicable dans la réalité.

Pour **Auguste Kerckhoffs, la sécurité d'un système de chiffrement ne doit reposer que sur la clé**. Selon lui, pour un système de chiffrement sécurisé, il faut diffuser les algorithmes, la façon dont le message est chiffré, sans en donner la clé. C'est ce principe qui est aujourd'hui retenu pour envoyer des messages cryptés, dans un contexte où l'échange de messages se fait entre de nombreux interlocuteurs et le partage de clé n'est plus sécurisé. Des outils mathématiques, les fonctions à sens unique, ont permis de répondre au principe de Kerckhoffs. C'est ce qu'on appelle les **fonctions à sens unique** : **à partir d'un antécédent, on est tout à fait en mesure de calculer l'image, mais la réciproque est très compliquée, sauf à connaître une « brèche secrète » qui rend plus simple le calcul de l'antécédent.**

Finalement, les principes d'un système de cryptographie sont : un chiffrement pour l'émetteur simple et rapide, un déchiffrement par le récepteur simple et rapide, un décryptage difficile et long pour un intrus, et le respect du principe de Kerkhoffs, sans partager sa clé.

La factorisation de nombres premiers est présentée comme exemple de fonction à sens unique, c'est sur cet outil mathématique qu'est construit le système de chiffrement RSA très utilisé par les entreprises, notamment pour le commerce électronique. Les **applications à sens unique utilisées en cryptographie dépendent d'une clé publique et d'une clé privée**. **Le chiffrement s'obtient en se servant simultanément de la clé publique et de l'application**. **La brèche secrète que comporte l'application constitue la clé privée, utilisée pour le déchiffrement**.

L'algorithme de Hachage emprunte la même logique de fonction cryptographique à sens unique. La fonction de hachage à sens unique (SHA256 pour la plus récente) crée un condensé du message et réduit le document, de quelque nature qu'il soit, à une empreinte numérique à sens unique (le « hash »). Il suffit de changer une lettre ou une minuscule en une majuscule au document, pour que le résultat soit totalement différent, ce qui permet de dire que le hash garantit une empreinte numérique à sens unique. L'authentification de l'émetteur peut être garantie par l'application de sa clé privée sur un en-tête de message. La clé publique, elle, permet à chacun de contrôler en déchiffrant la signature.

La blockchain, est alimentée au fil de l'eau par l'ensemble des nœuds du réseau, qui vont regrouper les transactions dans des blocs. **Un bloc est un groupe homogène de transactions**. Chaque nouvelle transaction est incrémentée sous forme de bloc, qui est soumis, validé et diffusé sur le réseau, puisque tout le monde doit avoir le même registre.

Le contenu d'un bloc est soumis à une fonction de hachage pour obtenir son hash (unique et imprédictible). Le hash est ensuite intégré au bloc suivant et sera soumis à une fonction de hachage avec le contenu de ce nouveau bloc, pour obtenir un nouveau hash.

Le minage consiste, pour le nœud, à faire sa preuve de travail, sous forme de problème mathématique complexe à résoudre (ex : déchiffrer un code calculé à partir d'une fonction à sens unique) pour pouvoir soumettre et valider son bloc.

Un des nœuds du réseau, le **« mineur », doit être en mesure de résoudre l'équation cryptographique,** qui représente la preuve de sa production de travail, et la soumettre aux autres nœuds du réseau, qui vérifient son résultat. Il peut arriver, sur un réseau de dizaines de milliers de nœuds, que des validations concurrentes arrivent au même moment. Dans ce cas, le protocole garde la chaîne la plus longue.

Le côté infalsifiable vient de la logique des blocs. En cas de modification d'un bloc, c'est toute la chaine des hash qui devient caduque, ce qui est immédiatement repéré par les nœuds du réseau. **La fonction de hachage maintient donc l'intégrité de la chaîne des blocs**

L'histoire du Bitcoin

Le bitcoin a été la première blockchain, née d'un mouvement anarcho-capitaliste, qui défend la liberté de faire des investissements sans contrôle d'Etat ni contrôle financier. Son créateur officie sous le pseudonyme de Satoshi Nakamoto (dont certains affirment qu'il s'agit d'un collectif de plusieurs personnes) qui a rédigé un livre blanc d'une dizaine de pages présentant les concepts principaux du bitcoin. Lancé en 2009, le système repose sur la logique des blocks, et des hash et n'a toujours pas été craqué. Il utilise des systèmes de clés publiques et privées : **la clé publique est l'adresse du compte sur lequel peuvent être faits les dépôts** et **la clé privée permet de dépenser les sommes présentes sur le compte**. La blockchain du bitcoin garantit une pseudonymisation, puisque les acteurs sont identifiés par une clé. Il est par ailleurs possible de générer autant de clés qu'on le désire.

Sur la chaîne du bitcoin, le problème est dimensionné pour que des blocs soient générés toutes les 10 minutes environ. Cependant, le nombre maximum de bitcoins est limité à une vingtaine de millions, ce qui rend inéluctable l'arrêt du système**. La rémunération incitative du minage est associée aux frais de transaction fixés par les utilisateurs pour que des mineurs ajoutent leur transaction au réseau**. Par ailleurs, une **rémunération liée au processus de création monétaire** de bitcoin est prévue par le protocole en cas de création de bloc, mais son montant décroît exponentiellement et devrait tomber à 0 en 2140. Plus le temps passe, plus le minage est difficile et concurrentiel, impliquant une consommation importante de CPU et d'électricité et aujourd'hui, il est par conséquent réalisé dans quelques fermes de minage à la puissance de calcul très importante, principalement situées en Chine, et qui en réalisent près de 51%, mettant ainsi à mal le modèle original.

Plusieurs modèles de blockchain

La blockchain publique, telle qu'elle a été décrite précédemment, est une blockchain accessible à tous dans le monde, à laquelle chacun peut envoyer des transactions, et s'attendre à ce qu'elles soient incluses dans le registre, pour peu qu'elles en respectent les règles. Elles sont sécurisées par la combinaison de la cryptographie et d'incitations économiques à la vérification des transactions.

Le smart contract est un programme autonome qui, une fois démarré, exécute automatiquement des conditions définies au préalable et inscrites dans la blockchain. Il existe des projets et quelques cas d'usage concernant l'assurance récolte ou le retard d'avion. Par exemple, un vol en retard génère automatiquement le versement d'une prime de dédommagement. Un assureur, ici AXA, peut s'appuyer sur une blockchain pour offrir ce service, à une compagnie aérienne, avec pour client final le passager.

La blockchain de consortium se différencie par un processus d'approbation contrôlé par un nombre restreint et choisi de nœuds, Par exemple, une quinzaine d'institutions financières pourraient se mettre d'accord et organiser une blockchain dans laquelle un bloc devrait être approuvé par au moins dix d'entre elles pour être valide. L'accès au registre peut alors être public, réservé aux participants ou hybride. L'appellation « blockchain » est assez contestable, dans la mesure où dans la blockchain, le registre est censé être ouvert à tous, chacun pouvant y participer. C'est également supprimer la notion de tiers de confiance, dès lors que l'on crée une forme de contrôle sur ces blockchains.

La blockchain privée est une blockchain de consortium appliquée aux différentes entités d'une même entreprise ou organisation, afin de simplifier et de fluidifier les échanges intra-entreprise en substituant aux nœuds de contrôle des systèmes répartis. Elle permet de travailler sur des processus métier, comme dans le cas de B3i, un consortium d'assureurs menant un projet de réassurance (assurance d'un assureur). Un premier projet a été développé sur la plateforme d'IBM Hyperledger, qu'ils ont quittée pour la plateforme Corda. La partie finance se fait sur un mode anglo-saxon, avec la mise en production d'un système de transactions financières basées sur la blockchain, Ripple, soutenue

par les grandes banques. Une autre application en production de système blockchain concerne le suivi des trolleys de logistique, avec un suivi de localisation et de responsabilité.

Enjeux et avenir

Sur la courbe de Hype, selon le Gartner, la blockchain est passée par le pic des attentes exagérées et se trouve sur une pente descendante, même s'il n'a pas atteint le temps des désillusions. Il faut rester très prudent par rapport à ce que cette technologie peut offrir et les quelques cas d'usage existants, mais la promesse de la blockchain est réellement la désintermédiation de la confiance, cette confiance qui vaut aujourd'hui de l'or.

L'enjeu autour du contrôle des blockchains est une problématique à ne pas négliger. Une blockchain privée est-elle une blockchain ? Peut-on imaginer que certains acteurs s'engagent, à travers la blockchain, dans une logique de décentralisation pour ensuite mieux centraliser et contrôler, à l'issue d'un processus traditionnel de concurrence entre plateformes ?

Pierre BERLIOZ : les enjeux juridiques liés à la blockchain

L'enjeu juridique principal lié à la blockchain est celui du cadre réglementaire, avec la question : « Faut-il légiférer ? ». De manière générale, lorsque l'on voit apparaître une innovation, la question qui se pose immédiatement est celle de la nécessité de prévoir une loi. Doit-on l'encadrer ? Doit-on prendre un décret ? Une loi ?

Aujourd'hui, la réponse, lorsqu'on a été conseiller du Ministère de la Justice est « Surtout pas ! **Ne légiférons pas ou alors le moins possible !** ». On constate que les lois sont globalement mal faites, ainsi que les règlements et les décrets, car chaque partie prenante cherche et souvent parvient à intégrer son cas particulier dans la loi, ce qui conduit à de l'**empilement législatif** et des **lois totalement illisibles**. Le corpus législatif est très dense, avec plus de 60 codes en France, alors que le premier réflexe des juristes consiste en réalité à chercher les solutions dans un cadre législatif et un cadre réglementaire existants qui seraient suffisamment accueillants pour adopter les nouveaux objets et les régir de façon souple.
En matière de blockchain, comme dans tous les autres domaines des nouvelles technologies, le point crucial consiste à ne pas légiférer trop vite, pour éviter de bloquer l'innovation. Légiférer oui, mais lorsque l'on connaît l'objet, ses impacts et que l'on est susceptible de savoir si le droit répond aux enjeux ou pas. C'est uniquement s'il n'y répond pas que l'on doit légiférer.

En droit, aujourd'hui, on utilise un **nouvel instrument qui est le droit souple**.
Le droit dur, de manière générale, consiste en une règle de comportement et une sanction si la règle n'est pas respectée. **Le droit souple**, en revanche, est une règle sans sanction, notamment une règle que l'on va se donner soi-même. La logique de RSE (Responsabilité Sociale et Environnementale ou Responsabilité Sociétale de l'Entreprise), par exemple, concerne une entreprise vertueuse qui se donne à elle-même un certain nombre de règles qu'elle décide elle-même de respecter, et cela pour aller au-delà de la loi. L'avantage du droit souple est qu'il peut être adapté en piochant dans les bonnes pratiques. En matière de nouvelles technologies, c'est très utile, car cela permet de créer un corpus que l'on s'engage à respecter, qui va finalement s'appliquer par la référence commune, par la pression qu'il peut y avoir à l'adopter mais sans sanction juridique.

Voici trois exemples de cas d'usage de la blockchain, dont certains font déjà l'objet de textes, alors que d'autres pas.

Les ICO, que l'on a nommés ainsi en référence aux IPO (appels publics à l'épargne avec mise sur le marché de titres de capital, actions ou parts sociales), en reprennent le principe en l'appliquant au domaine des crypto actifs. Dans le cas des ICO, des « token », c'est-à-dire des jetons, qui peuvent représenter un service, un bien, un droit au capital, une créance, un droit de vote, etc , sont attribués en échange de crypto-actifs comme du bitcoin ou de l'ether. L'ICO passe par la blockchain et permet de lever des fonds extrêmement rapidement (de l'ordre de 60 millions d'euros en une nanoseconde), grâce notamment à la possibilité de s'adresser au monde entier pour réaliser des transactions. L'ICO est très complexe à encadrer juridiquement car il se rapproche de plusieurs figures juridiques : de l'IPO, encadré par la réglementation appliquée aux marchés boursiers ; de l'échange ; et parfois de la vente. En réalité, en fonction du type d'opération, ce sont des réglementations très différentes qui s'appliquent, d'où une grande prudence nécessaire pour les encadrer, comme en atteste une consultation lancée par l'AMF (Autorité des Marchés Financiers).
Pour les ICO, qui ressemblent à des appels publics à l'épargne, la solution retenue et intégrée dans le projet de loi Pacte est de type droit souple. Il s'agit de ne pas fixer légalement de réglementation, mais de demander à l'AMF d'émettre un visa pour certifier que l'ICO correspond bien aux critères de l'appel public à l'épargne. On n'applique donc

pas directement la réglementation liée à l'IPO, mais on introduit un mécanisme de certification par une autorité qui a toute crédibilité pour sécuriser le marché, afin de ne pas freiner le développement d'initiatives originales intéressantes pour les appels de fonds. Cette réglementation a minima permet d'avancer progressivement alors que les ICO sont encore peu nombreux (une soixantaine en France).

Les registres de titres sont un autre cas d'usage de la blockchain, pour des entreprises qui souhaitent enregistrer les mouvements de parts de leur capital entre les différents associés. Pour cela, l'entreprise ou un tiers intermédiaire tient un registre des titres. Le législateur a considéré que l'on pouvait assimiler la blockchain à un registre de titres, à un registre des parts sociales et par conséquent, a ajouté le mot blockchain dans le code monétaire et financier pour entériner l'utilisation de la blockchain comme registre de titres. En revanche, le législateur n'a pas considéré qu'une opération qui est enregistrée dans la blockchain ne peut pas être remise en cause. En droit français, la question se pose pour le registre en lui-même, car on a plutôt tendance à considérer que l'inscription sur le registre n'est pas constitutive de la propriété de la part sociale, mais n'en est qu'une preuve. On n'a pas fait produire à la blockchain un effet plus fort, qu'aux autres registres. C'est la raison pour laquelle on ne peut pas dire que la blockchain permettra de remplacer les notaires. Elle peut servir à tenir le registre de la publicité foncière, qui enregistre toutes les ventes immobilières et permet d'en retracer l'historique de façon infalsifiable, car elle fournit un horodatage de l'inscription du document. Cette technologie sera d'ailleurs de plus en plus utilisée en matière de propriété intellectuelle, pour dater un processus de création et prouver une antériorité, afin de revendiquer un droit sur une création. En revanche, l'inscription dans la blockchain ne permet pas de montrer qu'un document correspond à la réalité de la transaction, ce qui est le rôle du notaire : il atteste de la volonté des parties de vendre et d'acheter. C'est la raison pour laquelle les notaires sont aujourd'hui en train de réfléchir à utiliser la blockchain pour développer un outil plus perfectionné de minutier central. Ils garderont toutefois la responsabilité de la partie authentification du contenu du document.

Les smarts contracts, autre application de la blockchain, ne sont ni des contrats, ni intelligents. Au contraire, il s'agit d'un système complètement mécanique. Le smart contract est un pur programme placé dans la blockchain, qui s'exécute et, par exemple, si un avion a plus de deux heures de retard, déclenche un remboursement de 200 euros. Le programme va chercher l'information là où elle se trouve, constate le retard et déclenche le paiement. Cela n'a rien d'intelligent et n'a rien d'un contrat, puisqu'il ne s'agit pas d'un accord de volonté. C'est uniquement une modalité d'exécution automatique du contrat, grâce à la garantie autonome, qui permet à la banque de l'emprunteur de s'engager à payer le prêteur sans discuter. Les problèmes rencontrés concernent plutôt les enjeux de restitution, dans les cas où le programme se déclencherait à tort, suite à une manipulation ou à une erreur dans la diffusion de l'information. Mais des textes existent pour gérer ce type de situation, et il suffit de les appliquer.

En matière de blockchain, comme dans beaucoup de secteurs, il ne faut pas légiférer trop vite ni trop réglementer, au risque de créer un dispositif qui bloquerait un certain nombre d'innovations. Il faut observer les usages, travailler à créer des bonnes pratiques et un encadrement volontaire au niveau sectoriel. **La bonne démarche est plutôt expérimentale** et consiste à rédiger des **chartes de bonnes pratiques**, que le législateur peut ensuite décider de généraliser quand elles ont fait leurs preuves.

Intervenant : Dans le cadre de la RGPD, comment satisfaire une demande d'effacement de donnée personnelle dans la blockchain ? Dans la blockchain, il n'y a pas d'oubli…

Pierre BERLIOZ : C'est le problème effectivement, le droit à l'oubli pose problème. D'où mon conseil de ne pas intégrer dans la blockchain des données personnelles. Après, tout ça s'enterre et se noie dans la masse…

Benjamin RAMEIX : Les bases de données de personnes peuvent rester au sein de l'entreprise. La blockchain peut tourner avec des identifiants et des clés. La solution peut résider dans le fait que la gestion des ID, les bases de données peuvent rester chez le partenaire.

Int. : Que voulez-vous dire par « ça s'enterre », « Noyer dans la masse » ? Est-ce que cela signifie que c'est trop compliqué à remonter ?

P. B. : Oui.

Int. : Comment imaginer la croissance de la blockchain publique ?

P. B. : En 2140, c'est la fin du bitcoin.

B. R. : Il existe plusieurs blockchains publiques : celle du bitcoin, celle de l'ethereum, etc… Mais aujourd'hui, le minage du bitcoin est très long : on est passé à plus de 10 minutes pour une inscription, alors que c'est beaucoup plus rapide pour des blockchains fondées sur Ethereum. On passe de l'une à l'autre, mais il existe un effet d'obsolescence. La question est difficile et il y aura probablement des conflits, des chaines qui prendront le pas sur d'autres, ou des acteurs qui vont prendre le lead, à l'image de ce qui a pu exister dans la net-économie.

Int. : Comme les blockchains sont supportées par les ordinateurs, elles ne peuvent pas vivre éternellement, alors que l'on cherche des registres qui durent dans le temps. On sait que c'est supporté par une technologie qui évolue toujours, donc il y a là quelque chose de gênant.

B. R. : Certes mais c'est un débat plus général, et avant cela le sujet de la consommation risque aussi d'être un vrai frein. On peut également mentionner le sujet de la sécurité de la partie….

Int. : Quel autre type de blockchain peut-on envisager dans l'assurance ?

B. R. : Les assureurs s'organisent en consortium (B3i) ou à travers leur fédération (FFA). Ce sont les blockchains de consortium ou privées. A défaut de révolution immédiate, la blockchain simplifiera les process car dans l'assurance et la banque, la donnée et l'information sont les matières premières des produits : nous sommes sur des enjeux de gestion de flux et d'interconnections de très nombreux systèmes. Je pense que ce type de technologie, surtout dans des logiques de consortiums, pourront déjà améliorer les process

P. B. : Et puis l'internet de l'objet. C'est l'interaction entre objet et la possibilité pour les objets de faire un certain nombre d'opérations, notamment le frigo qui vous commandera les yaourts directement quand il n'en restera plus qu'un. C'est du smart contract.

Int. : Est-ce qu'il y a besoin de faire l'économie d'un tiers de confiance, ou pas ? Par exemple, si les systèmes de paris sont interdits et que l'on met cela dans une blockchain, personne n'ira en prison, puisqu'il n'y a pas de tiers de confiance impliqué.

Int. : Et si quelqu'un arrive à mettre des informations fausses dedans, elles y restent parce qu'il n'y a pas d'huissier capable de les enlever…

B. R : Il existe aujourd'hui des huissiers qui développent des services de certification de documents qui seront ensuite mis sur la blockchain.

Int. : Est-ce qu'on sait qui investit dans le minage des blockchains ? Est-ce que c'est rémunérateur ? Est-ce qu'il y a des noms connus ?

B. R. : Les mineurs sont des pools chinois. Sur le bitcoin, il y en a quatre ou cinq qui dominent. Il existe une mappemonde où l'on voit les pools de minage, que vous pourrez trouver sur le net On y voit le poids de la Chine. L'Europe est assez active aussi.

P. B. : C'est rémunérateur là où l'énergie ne coûte pas cher.

Int. : Le droit à l'oubli est encore plus mis à mal dans les consortiums, car il est plus facile d'y retrouver des données.

B. R : Dans un consortium, on a un regroupement, d'assureurs par exemple, qui ont chacun leur base clients. A eux de décider comment ils s'organisent sur la gestion des personnes. S'ils ne partagent pas leurs bases, ils peuvent passer par des identifiants, par des clés de rapprochement pour anonymiser la donnée.

Int. : Dans l'assurance, dans le cadre des conventions de gestion de certains risques, on est bien obligé de balader des données personnelles.

Int. : Tout dépend si le document reste extérieur et que l'on a juste le hash dans le bloc.

B. R. : Dans des flux inter-assureurs, tout dépend des conventions passées entre ces assureurs. On ne donne pas forcément les identifiants clients.

Int. : Il y a bien le nom de conducteur, son numéro de contrat, etc, dans la transaction à enregistrer.

B. R. : Cela pourrait ne pas être le cas, car sinon cela veut dire que l'on utilise la blockchain comme une base de données client. Il faudrait les conserver à côté, dans son SI sécurisé, pour y accéder tant que de besoin. Le registre a initialement vocation à stocker des transactions, pas des bases client type ERP. Dès lors, c'est la convention entre assureurs qui détermine ce qui doit et peut être échangé. Sur une blockchain privée d'entreprise, elle est libre d'y véhiculer les données qu'elle souhaite.

Int. : Dans les cas d'usage d'un consortium, il n'y a aucun rapport entre ces technologies blockchain et les crypto-monnaies ? On se trouve juste dans une logique où l'on utilise la technologie pour faire des registres distribués indépendamment de toute logique de crypto-monnaie.

B. R. : Oui, c'est totalement indépendant.

Int. : Y compris dans un cas de consortium, si le système, la plateforme ne fonctionne plus, qui est responsable ?

P. B. : Sur un consortium à l'instar d'un SI mutualisé, et si c'est une blockchain publique, la résilience du réseau fait que la question ne se pose pas.

Int. : Quand il y a une monnaie, il y a toujours une banque centrale derrière. Là, il n'y a pas l'équivalent de la banque centrale. Si ça ne marche pas, qui est responsable ?

B. R. : De nombreuses banques centrales, de par le monde, considèrent qu'il est erroné de parler de crypto-monnaie. Elles préfèrent parler de crypto-actifs, c'est-à-dire, des supports de valeur qui ne sont pas des monnaie (des instruments de paiement ayant cours légal), car l'assise propre aux monnaies qui permet une conversion sûre n'existe pas.

Int. : Il s'agit donc plutôt d'une place boursière que d'une monnaie.

P. B. : Voilà ! On est plus sur une valeur qui est fonction de l'offre et de la demande. C'est pour cela qu'il vaut mieux parler de crypto-actif que de crypto-monnaie. Sur la question de la responsabilité, on revient sur les fonctionnements habituels du droit de la responsabilité : tout dépend de l'origine du bug. Si on a un défaut dans la conception de l'outil, on ira chercher le fabriquant. Si on a un problème dans la manière dont on l'a utilisé, on ira chercher l'utilisateur. La question de la responsabilité est plus compliquée en matière d'intelligence artificielle, mais sur la blockchain, on peut facilement appliquer les mécanismes de droit commun.

Présentation des orateurs

Benjamin RAMEIX est membre de l'ANDSI depuis huit ans. Ingénieur ENSMA de formation, et diplômé de l'EN3S, il a débuté sa carrière par trois années de consulting puis chez Groupama. Toujours dans le secteur de la protection sociale et de l'assurance de personne, il a été successivement DSI de la Caisse des Français de l'Etranger puis de la mutuelle Unéo. Il est aujourd'hui le DSI du Groupe PREVOIR.

Pierre BERLIOZ est Professeur de droit et Directeur de l'école de formation des barreaux. Il est spécialiste du droit des actifs immatériels et du droit patrimonial de l'entreprise, en droit interne et international et ancien conseiller du Garde des Sceaux.