Université Paris Est Créteil

Master 2 Droit de la propriété intellectuelle appliquée

Dirigé par le Professeur Christophe Caron

2017-2018

LA BLOCKCHAIN ET LA PROTECTION DES DONNÉES PERSONNELLES

Présenté par Audrey SIDE, Benjamin MOLLET-VIEVILLE, et Augustin CORDIN

Sous la direction de Madame Iris M. BARSAN, maitre de conférences en droit des nouvelles technologies au sein du Master 2 PIA

Encadré par Maître Magalie DANSAC LE CLERC, Partner chez Baker & McKenzie

Nous tenons avant tout à remercier Madame Iris M. Barsan, pour l'initiative ainsi que l'énergie consacrée à l'organisation et la réalisation de ce passionnant projet, qui n'aurait pas été possible sans elle.

Nous remercions chaleureusement Maître Magalie Dansac Le Clerc d'avoir accepté d'encadrer notre travail, et d'y avoir consacré son temps afin de nous prodiguer ses précieux conseils.

Nous remercions également le cabinet d'avocats Baker & McKenzie de nous avoir fait l'honneur de participer à ce projet, et de nous accueillir dans ses locaux afin que nous puissions leur présenter cette étude.

Nous remercions par ailleurs Monsieur Sébastien Madet, consultant en cyber sécurité chez Harmonie Technologie, d'avoir pris le temps de répondre à nos questions, et de nous avoir livré son expertise en matière de blockchain et de sécurité des données.

Nous remercions enfin Monsieur le Professeur Christophe Caron, directeur de notre Master, de nous avoir permis de participer à cette expérience si enrichissante.

Préface

La technologie blockchain

En mai 2017 la directrice du fond monétaire international déclarait qu'elle voyait dans la blockchain « une plateforme idéale pour discuter des évolutions technologiques dans le domaine de la finance ». Emmanuel Macron alors qu'il était encore ministre des finances était également déjà en faveur de l'adoption d'une « blockchain à la française » et pour son utilisation notamment pour le financement participatif.

L'évolution de la blockchain comme support technique des cryptomonnaies semble donc se démocratiser même si aucune législation n'est encore existante sur ce sujet. Elle s'est notamment faite connaître à travers la cryptomonnaie Bitcoin. Là où certains voient dans les cryptomonnaies et la blockchain la fin d'un système capitaliste organisé et d'un ordre établi, il convient de définir ce qu'est la blockchain et d'établir quel est son fonctionnement.

La blockchain est une technologie qui permet de stocker, transmettre et échanger des informations. Elle a été développée dans le but d'être accessible et modifiable par tous, sans nécessité de faire appel à un intermédiaire pour superviser les informations échangées en son sein.

C'est une base de donnée qui retranscrit et rend intelligible toutes les transactions de ses utilisateurs depuis sa création. Les caractéristiques principales de la technologie blockchain sont qu'elle fournit une traçabilité de toutes les transactions passées, l'intégrité des informations échangées est garantie et il n'y a pas d'intermédiaire.

La blockchain est organisée en plusieurs blocs de transactions. Chaque bloc se forme environ toutes les dix minutes et est relié au précédent.

Les transactions sont constituées d'une adresse publique émetteur, d'une adresse publique du/des destinataires, du montant de la transaction et des frais de transaction.

Chaque bloc comporte enfin un entête appelé « hash » qui servira d'identificateur du bloc car il contient la date et l'heure du bloc ainsi que le hash du bloc précédent, ce qui rend sa modification impossible.

Le fonctionnement de cette technologie repose principalement sur les mineurs qui sont des personnes chargées d'effectuer des opérations de validation d'un ensemble de transactions à l'intérieur d'un bloc. Ils mettent à disposition la puissance de calcul de leur matériel informatique. Cette opération caractérise le minage.

Il existe différents types de mineurs : les mineurs dit particuliers qui investissent dans un matériel comportant une très grande puissance de calcul ; les pools de mineurs qui sont un ensemble de mineurs qui rassemblent leur puissances de calcul afin d'augmenter leurs chances de miner un bloc ; et enfin les mineurs professionnels qui sont une entreprise de minage qui développe des techniques permettant d'optimiser un matériel informatique.

Le minage constitue un challenge pour les mineurs, ils sont mis en compétition et sont rémunérés en cryptomonnaies.

Le *token* correspond à un actif numérique permettant à une transaction d'être effectuée au sein de la blockchain. C'est une unité monétaire qui peut être transférée entre deux parties, tout comme c'est le cas du bitcoin.

Il existe deux grands types de blockchain : la blockchain publique et la blockchain privée.

La blockchain publique est caractérisée par le fait qu'elle se matérialise sous forme de registre public : n'importe quel utilisateur dans le monde peut la lire, lui envoyer des informations et y passer des transactions qui seront inscrites dans le registre. C'est le cas par exemple de la blockchain Bitcoin qui est une blockchain publique et à laquelle chacun peut avoir accès.

La deuxième caractéristique de la blockchain publique est qu'elle est soumise à un processus de validation des blocs ouverts à tous, appelé le minage. N'importe quel utilisateur (à condition de disposer de la puissance de calcul nécessaire) peut librement participer à ce processus et approuver les transactions effectuées dans la blockchain.

Concernant la blockchain Bitcoin par exemple, à moins de disposer d'au minimum 51% des ressources utilisées pour le bitcoin, pour ainsi avoir le droit de miner tous les blocs, il est impossible de falsifier ou inscrire de fausses informations dans une blockchain publique.

La blockchain privée est quant à elle caractérisée par le fait qu'elle se matérialise sous la forme d'un registre public ou privé. Cela signifie que la consultation de ce registre peut être en fonction des cas publique ou privée. Le processus de validation des blocs est limité à un nombre restreint de personnes appelées consortium, qui peut même être une seule personne dans le cas où il n'y aurait qu'un seul nœud. Cette blockchain, contrairement à la blockchain publique, est donc beaucoup plus facilement falsifiable compte tenu du petit nombre de mineurs qui peuvent s'entendre entre eux sur les informations à intégrer à la blockchain.

Ce type de blockchain peut être critiqué car elle remet en cause les principes fondateurs de cette technologie, à savoir l'intégrité et la décentralisation.

Introduction

Rendue célèbre par le Bitcoin, cette technologie attire aujourd'hui de plus en plus les opérateurs économiques. Banque, finance, gestion des droits de propriété intellectuelle, état civil, santé… Les acteurs de nombreux secteurs y voient un « paradigme organisationnel »[1], leur promettant une meilleure traçabilité, transparence, et efficacité de leurs opérations.

Dès lors, difficile de ne pas évoquer la question du sort réservé aux données manipulées via cette application. En effet, la blockchain a vocation à révolutionner la perception actuelle du traitement des informations, en proposant de les transmettre et de les stocker sur un registre consultable par tous, décentralisé, et dont tous les membres permettent d'en assurer la fiabilité[2]. Toutefois, aussi innovante et « disruptive » soit-elle, il n'en reste pas moins vrai que l'utilisation de cette technologie peut, directement ou indirectement, impliquer des données à caractère personnel. Dans son application pratique, la blockchain ne peut donc pas occulter ce droit fondamental à la protection des données des personnes concernées. Plus encore, c'est dans l'intérêt même des acteurs prônant ses bienfaits de démontrer que ce mécanisme est digne de confiance.

Or à l'heure où de nombreuses entreprises tentent tant bien que mal de se conformer au nouveau règlement général sur la protection des données (ci-après « RGPD »)[3], applicable dès le 25 mai prochain, leur volonté émergente d'utiliser une telle technologie s'avère être un défi de taille.

La première raison à cela tient au fait que le RGPD, pourtant rédigé en vue de s'adapter aux évolutions technologiques et à l'ampleur prise par la collecte et le partage des données personnelles, n'a pas été pensé pour tenir compte de la technologie blockchain.

---

[1] Dominique Legeais, Fasc. 534 : BLOCKCHAIN, JurisClasseur, 7 mars 2017, n° 10

[2] Blockchain France, *Qu'est-ce que la blockchain ?*
https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/

[3] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

En effet, le droit français peut par exemple se targuer d'avoir récemment pris en compte l'existence de la blockchain en droit financier, en la définissant par cette occasion comme un « *dispositif d'enregistrement électronique partagé* »[4]. Or malgré l'impact considérable que pourrait potentiellement avoir cette technologie de stockage et de transmission d'informations transparente et décentralisée en matière de traitement des données personnelles, le RGPD n'a pas prévu de dispositions spécifiques, ou du moins une définition légale de la blockchain.

Pourtant, et comme nous le verrons en première partie, les grands principes posés par le RGPD ne semblent pas forcément adaptés à l'utilisation de cette technologie. Enfin, plus généralement, il se doit d'être souligné que si la manière de se conformer à cette règlementation générale a certes pris forme, force est de constater qu'il est encore impossible de savoir comment sera appliqué le RGPD en pratique.

De la même manière, le projet de loi relatif à la protection des données personnelles[5], récemment adopté par l'Assemblée Nationale[6], ne se prononce pas plus sur cette question. En effet, la loi n° 78-17 du 6 janvier 1978 relative à l'informatique et aux libertés, qui sera largement révisée à cette occasion, se devait de se conformer au nouveau règlement européen. Et force est de constater que ce projet opère pour le moment une réforme extrêmement fidèle aux dispositions du règlement.

Peut-on pour autant parler de rendez-vous manqué par le législateur français et européen ? Rien n'est moins sûr, car la difficulté d'appréhension de cette technologie vis-à-vis de la protection des données tient également au fait que la blockchain, bien qu'utilisée depuis 2009, est loin d'avoir livré tous ses secrets. En effet, au-delà des cryptomonnaies, force est de constater que l'usage de cette technologie dans le monde économique n'en est encore qu'à ses prémices.

[4] Ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers

[5] Projet de loi relatif à la protection des données personnelles (JUSC1732261L)

[6] Adopté en première lecture le 13 février 2018 par 505 voix contre 18, avec 24 abstentions

Il est donc aujourd'hui impossible de savoir concrètement de quelle manière elle sera précisément utilisée, et quel sera son impact en termes de traitement des données personnelles.

C'est la raison pour laquelle cette étude se basera avant tout sur la blockchain Bitcoin, dont la force de l'usage depuis maintenant près d'une dizaine d'années permettra d'avoir un exemple concret des conséquences de cette technologie, ainsi que du rôle exercé par les diverses parties prenant part à son application.

Et si l'hypothèse d'une règlementation spécifique est probable dans un futur relativement proche, la démocratisation imminente de la blockchain dans la « vie courante » des affaires nous invite avant tout à se demander comment tenter de la concilier avec ce qui sera, pour sûr, le droit positif de demain en matière de protection des données personnelles.

A cet égard, il sera tout d'abord intéressant d'étudier quels sont les obstacles à cette conciliation (I), avant de tenter d'analyser comment il serait possible de les résoudre, dans le but d'envisager un usage de la blockchain conforme, voire utile à la protection des données personnelles (II).

Table des matières

I. L'inadéquation du RGPD à la blockchain

La protection des données personnelles constitue en France et en Europe un droit fondamental. Cette protection est garantie en France par l'article 9 du Code civil et par l'article 2 de la déclaration des droits de l'homme de 1789. Le Conseil constitutionnel l'a érigée en valeur constitutionnelle dès 1995 à l'occasion d'un contrôle de constitutionnalité de la loi encadrant les autorisations d'installation de systèmes de vidéosurveillance[7]. A l'échelon européen, la protection des données personnelles est garantie par l'article 8 de la CEDH et de manière encore plus précise par l'article 8 de la charte européenne des droits fondamentaux. La Cour de justice et la Cour européenne saisissent régulièrement l'occasion de rappeler l'intérêt supérieur de cette protection[8].

Revendiquant l'héritage de la loi française « informatique et libertés » de 1978 maintes fois modifiée, le législateur européen a précisé dans le règlement général sur la protection des données (RGPD) les conditions de traitement des données personnelles. C'est à la lumière de ses dispositions ainsi que sur le projet de loi de son application en France que seront traitées les données personnelles.

A. Des enjeux antinomiques

1. Le traitement des informations

Les données personnelles sont envisagées par le droit à travers le prisme de leur protection. Elles sont une composante de la vie privée et appartiennent aux droits de la personnalité. En prenant connaissance des données personnelles d'un individu, on tend à se rapprocher de son essence : ses caractéristiques physiques, son statut social, son image, ses habitudes de consommation, ou encore sa réputation.

[7] Décision n° 94-352 DC du 18 janvier 1995
[8] Notamment, CEDH, 5 septembre 2017, Barbulescu c/ Roumanie

La « blockchain » est un moyen technologique qui vise un tout autre objectif. Elle vise à garantir l'authenticité d'une information (qu'elle qu'en soit sa nature) par son partage au plus grand nombre. Cette technologie s'inscrit dans une évolution sociétale qui tend à promouvoir le partage de l'information. Cette évolution se traduit par l'essor des réseaux sociaux, les logiciels en licence libre ou les réseaux de pair à pair.

Si la blockchain doit contenir en son sein des informations personnelles, son réflexe premier sera de les partager. La transparence des informations qu'elle héberge constitue le projet originel de son mystérieux concepteur, Satoshi Nakamoto. Sans transparence, sans partage, sans diffusion au plus grand nombre possible, la blockchain perd son aptitude à garantir à tous l'intégrité de l'information.

La blockchain veut partager les informations, le RGPD veut les protéger : c'est le premier enjeu antinomique.

2. Le détenteur des informations

La blockchain part d'un constat sur le fonctionnement de notre société. Pour assurer un échange de biens, de valeurs ou d'informations, nous avons besoin de tiers de confiance. Ainsi, un notaire garantira la propriété réelle de chacun, une banque assurera un échange de valeurs, un réseau social transmettra un échange d'informations, etc…

La blockchain promet une désintermédiation. Il ne serait nullement nécessaire de confier à un tiers de confiance le soin de certifier ces échanges. En les partageant entre tous ses utilisateurs, la blockchain pourrait ainsi garantir l'authenticité de l'information transmise. Les échanges deviennent alors moins coûteux et plus rapides.

Le RGPD pour sa part accorde une grande importance au responsable du traitement des données personnelles. Il est l'objet de toutes les attentions du règlement. Ses obligations sont nombreuses et sa responsabilité est envisagée jusqu'à celle de son sous-traitant. Au même titre qu'il ne peut y avoir de protection des données personnelles sans données personnelles, il ne peut y avoir de protection des données personnelles sans responsable du traitement. Or, celui-ci s'apparentera dans bien des cas au tiers de confiance que la blockchain envisage de supprimer.

La blockchain veut supprimer le tiers de confiance, le RGPD par l'identification du responsable du traitement en fait un acteur principal : c'est le deuxième enjeu antinomique.

3. La conservation des informations

La blockchain par son architecture repose sur un registre exponentiel où la place de chaque information conditionne l'existence authentique de toutes les autres. On ne peut retirer une seule des informations contenues dans la chaine sans démonter toutes les autres informations. Les informations contenues dans la blockchain sont un tout indivisible. On ne peut les falsifier, les rectifier, les effacer. C'est un principe d'immutabilité que met en place la blockchain.

Le RGPD pour sa part, attache une très grande importance à une conservation limitée des données. Celles-ci doivent être effacées lorsqu'elles ne présentent plus d'intérêt direct pour celui qui les conserve.

Par ailleurs, le RGPD garantit au propriétaire des données personnelles le droit d'y avoir accès, de les rectifier et même de les supprimer. Ce droit fait l'objet de nombreuses dispositions relatives à ses principes, son fonctionnement et éventuellement ses sanctions.

La blockchain veut rendre les informations immuables, le RGPD veut les rendre temporaires et modifiables par le sujet des informations : c'est le troisième enjeu antinomique.

4. La valeur marchande des informations

Le RGPD, affiche la volonté de protéger l'individu de l'utilisation commerciale de ses données personnelles. En réalité, le RGPD définit un cadre légal à la transmission onéreuse des données personnelles. Il prend en compte la valeur marchande grandissante des données personnelles pour les opérateurs économiques. Le marketing ciblé et le traitement d'un grand nombre de données (Big Data) ont pris une place considérable dans le marché actuel à tel point que certains qualifient les données personnelles de « nouvel or noir ». Sous couvert de protéger les individus de l'utilisation trop sauvage de leurs données, le RGPD régule et organise un marché économique.

La blockchain, pour sa part, n'envisage pas la donnée comme une valeur en tant que telle. Elle ne protège pas les données, elle les authentifie, les certifie, non pas en les protégeant dans un coffre-fort mais au contraire en l'offrant au plus grand nombre. Sa valeur n'est pas patrimoniale, elle est le bien de tous.

Le RGPD reconnaît aux données personnelles une valeur, la blockchain veut les rendre gratuites : c'est le quatrième enjeu antinomique.

B. L'applicabilité partielle du RGPD au sein de la blockchain

Si l'on veut appliquer le RGPD à une blockchain, il convient d'isoler les deux éléments fondamentaux suivants : d'une part, les données personnelles et d'autre part, le responsable du traitement.

1. Les données personnelles

Quelles sont les données personnelles contenues dans une blockchain ? Il devrait exister autant de réponses qu'il y a de blockchains. En effet, selon le rôle conféré à la blockchain, les données personnelles diffèrent. Néanmoins, on peut distinguer deux données personnelles récurrentes : l'identité de l'utilisateur d'une part et d'autre part l'information que la blockchain a pour mission de conserver.

a) L'identité de l'utilisateur

En premier lieu, l'identité de l'utilisateur est dévoilée dans la blockchain. Lorsqu'une information est inscrite dans un bloc de la blockchain, elle se rapporte à un utilisateur. Par exemple, lorsqu'une transaction est inscrite sur la blockchain Bitcoin, il est mentionné un transfert de valeur entre un utilisateur A et un utilisateur B. Il est vrai que l'identité dévoilée de A n'est pas celle de son état civil. Il s'agira de son identité numérique propre à la blockchain. Cette identité prendra la forme d'une « clé publique », c'est-à-dire une suite très importante de chiffres. On retrouve ici le concept d'identifiants, de RIB, de numéro de sécurité sociale, d'adresse IP.

Qualifier la clé publique de donnée personnelle suppose de relier ce code à une personne physique. C'est ce qu'a jugé la Cour de cassation en 2016, à propos des adresses IP, en indiquant que « les adresses IP, qui permettent d'identifier indirectement une personne physique, sont des données à caractère personnel »[9].

Ainsi, le simple fait de pouvoir lier directement ou indirectement une personne physique à un code transforme ce dernier en donnée personnelle. Certes, on peut imaginer que les utilisateurs d'une blockchain cherchent à rester anonymes. Mais cette conception est purement théorique, car il s'agit à un moment ou à un autre d'inscrire dans la blockchain des opérations réelles. Un commerçant qui accepte les bitcoins sera forcément identifié par son client qui le payera dans cette monnaie. Inversement, le commerçant connaîtra forcément l'adresse du client à qui il devra livrer un objet (matériel ou immatériel). Ainsi, la blockchain dévoile inévitablement des données personnelles mais elle recèle également des informations sur l'échange en lui-même.

b) L'information que la blockchain a pour mission de conserver

Si l'identité de l'utilisateur peut s'avérer difficilement individualisable, l'information en elle-même est forcément visible sur la blockchain. Elle constitue l'essence même de la blockchain : inscrire une information authentique dans un grand livre numérique. Ce qui sera inscrit dans la blockchain sera visible de tous. Dans le cas de la blockchain Bitcoin, tous les utilisateurs pourront prendre connaissance des transactions et de leur montant. Un commerçant en Bitcoin pourra connaitre les transactions effectuées par ses clients, par ses concurrents. La connaissance des habitudes de consommation constitue le cœur même de la donnée personnelle utile.

C'est celle-là même que recherche les services marketing, bien plus encore que l'identité ou l'adresse physique du consommateur. En utilisant les puissances de calcul engendrées par le *big data*, l'opérateur économique aurait à portée de main une multitude de renseignements sur les différentes transactions réalisés sur la blockchain.

[9] Cass. 1ère civ., 3 nov. 2016, n° 15.22-595

Si la démonstration est évidente pour la blockchain Bitcoin, elle l'est tout autant pour toutes les blockchains. Ces dernières contiendront toujours une information personnelle relative à un individu.

2. Le responsable du traitement

Si la caractérisation des données personnelles dans une blockchain ne soulève pas de réelles difficultés, l'identification du responsable du traitement relève de la science-fiction.

Le RGPD impose de désigner une personne physique ou morale. Or, une blockchain fonctionne sans responsable, sans administrateur. La blockchain consiste en un logiciel qui fonctionne à la manière d'un robot programmé pour inscrire en son sein des informations. On pourrait être tenté de se tourner vers le créateur du code informatique. Mais, on se heurterait à un grand nombre de difficultés. Le créateur ne se sera pas forcément manifesté. Le cas n'est pas d'école. Personne ne sait à l'heure actuelle qui est réellement Satoshi Nakamoto, l'autoproclamé inventeur de la première blockchain sur les bitcoins.

Il faut ensuite rajouter un degré dans la difficulté : la plupart des blockchains, si ce n'est la totalité sont basés sur des codes en open source, rendant son origine encore plus inatteignable.

Un autre acteur pourrait incarner le responsable du traitement. il s'agit des mineurs, chargés de valider les blocs d'informations dans la blockchain. Il s'agit, pour la plupart, d'immenses hangars abritant des milliers de processeurs délivrant leur puissance de calcul à la blockchain. Si techniquement, on pourrait qualifier leurs opérations de traitement, à travers notamment la collecte de données personnelles, leur désintérêt pour la finalité du traitement apparaît totalement étranger à la conception de responsable du traitement du RGPD.

Si le responsable du traitement n'est ni le logiciel, ni son concepteur, ni les mineurs, on pourrait le désigner par l'ensemble des utilisateurs. Aucune des dispositions du RGPD n'empêche une pluralité de responsables. Bien au contraire, il l'envisage de manière très précise en encadrant les cotraitants et les sous-traitants. La pluralité n'est donc pas une réelle difficulté en soi.

Néanmoins en considérant que l'intégralité des utilisateurs sont des responsables de traitement, les obligations définies par le règlement à l'égard des responsables du traitement seraient démultipliées en autant d'utilisateurs peu enclins à se voir attribuer la responsabilité de l'intégralité du traitement des données personnelles.

Ainsi, appliquer le RGPD à la blockchain elle-même telle qu'elle a été conçue à son origine supposera d'interpréter et d'étendre les concepts définis par le règlement.

En revanche, le RGPD retrouve toute sa clarté lorsqu'il s'agit de l'appliquer à des opérateurs agissant en tant qu'intermédiaires entre la blockchain et ses utilisateurs.

II. Les solutions envisageables

Si la technologie blockchain ne semble pas pouvoir en elle-même remplir les conditions d'application du RGPD, il semble retrouver toute sa clarté lorsque des opérateurs agissent en tant qu'intermédiaires entre la blockchain et ses utilisateurs.
L'inclusion de ces acteurs de la blockchain pourrait en effet permettre l'applicabilité du RGPD.

Il conviendra également d'analyser les utilisations de la blockchain qui seraient susceptibles de confluer dans le sens du RGPD et de permettre une protection des données personnelles plus accrue.

A. La responsabilité des intermédiaires

1. L'applicabilité du RGPD aux intermédiaires

Le principe fondateur de la blockchain est la désintermédiation, mais il existe tout de même des acteurs qui permettant l'utilisation de cette technologie et finissent par remplir le rôle d'intermédiaires. On les retrouve notamment, au moment d'effectuer une transaction d'achat de cryptomonnaie, car ils sont chargés de faire le lien entre l'utilisateur de la cryptomonnaie et les plateformes d'échange.

L'enjeu de l'étude de la blockchain et du RGPD sera donc de savoir si le RGPD est applicable aux intermédiaires de traitement permettant l'utilisation de la blockchain. Cette question soulève plusieurs autres questions inhérentes à l'applicabilité du RGPD.

Qui sont les intermédiaires de la blockchain ?

Il convient tout d'abord d'identifier précisément et de manière pratique qui sont les intermédiaires techniques de la blockchain et quel est leur rôle.

Pour cela, une expérience pratique a été réalisée afin de connaître les étapes permettant à un utilisateur de la blockchain de l'utiliser via ces intermédiaires techniques.

La blockchain Bitcoin étant la plus connue, c'est celle qui a été choisie pour illustrer cet exemple. Il existe deux formes d'intermédiaires : les plateformes d'achat et les plateformes de transactions financières ou de trading.

Concernant les plateformes d'achat de bitcoins, une personne qui désire acheter des bitcoins dispose de deux possibilités pour le faire : elle peut se rendre dans un magasin physique tel que la Maison du Bitcoin, ou utiliser une plateforme internet comme par exemple *Coinbase*.

Concernant les plateformes de transaction financières, elles permettent la vente et l'achat de cryptomonnaies et peuvent être comparées à des traders boursiers. La plateforme la plus connue pour la cryptomonnaie se prénomme Kraken et recense en temps réel le cours de chaque cryptomonnaie ainsi que chaque blockchain correspondante.

Ces plateformes sont néanmoins interdépendantes, car la plateforme d'achat et de revente utilise la plateforme de transaction pour effectuer les transactions financières des acheteurs. En revanche il est possible d'utiliser la plateforme de transactions financières indépendamment des plateformes d'achat.

Ces mécanismes constituent donc un premier frein au principe fondateur de désintermédiation dont se prévaut la blockchain.

Quelles sont les missions des intermédiaires ?

Concernant la plateforme d'achat de Bitcoin, le futur acheteur devra lui fournir, pour effectuer une transaction, un certain nombre de données personnelles et notamment des données ayant un caractère d'identification de sa personne mais également des données permettant de le contacter ou encore de passer des transactions financières.

Ce transfert de données permet d'effectuer un premier rapprochement avec l'utilisation du RGPD, car si la question de l'applicabilité du RGPD se posait concernant la blockchain en tant que technologie car il semblait difficile d'identifier des données personnelles, la présence de données personnelles au stade des intermédiaires techniques ne semble faire aucun doute.

Dans l'optique de comprendre le cheminement de toutes ces données personnelles, l'intermédiaire technique physique "la Maison du Bitcoin" se trouvant au 35 rue du Caire, 75002 Paris a été choisie comme exemple.

La première étape d'achat des bitcoins consiste en la création d'un compte au sein du magasin de Bitcoin, à partir de données fournies par l'acheteur, et notamment la photographie de sa carte d'identité. En application de l'article 4-1 du RGPD, ceci constitue donc une donnée à caractère personnel.

Concernant la plateforme de transactions financières, sera chargée de veiller à la rencontre de l'offre et de la demande d'achat de bitcoins. Il est néanmoins impossible de déterminer à l'avance une transaction avec un utilisateur particulier car les transactions sont chiffrées et anonymes.

L'anonymisation est définie par le considérant 26 du RGPD comme les données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit plus identifiable.

La CNIL avait notamment eu l'occasion de rappeler à ce sujet que : *"pour qu'une solution d'anonymisation soit efficace, elle doit empêcher toutes les parties d'isoler un individu dans un ensemble de données, de relier entre eux deux enregistrements dans un ensemble de données (ou dans deux ensembles de données séparés) et de déduire des informations de cet ensemble de données"* à l'occasion d'un litige porté devant le Conseil d'Etat opposant la société JCDecaux à la CNIL.

Dans cette affaire, la CNIL avait en effet refusé d'octroyer à la société JCDecaux l'autorisation d'exploiter sur le parvis de La Défense un traitement automatisé de données à caractère personnel ayant pour finalité de tester une méthode d'estimation quantitative des flux de piétons. La société JCDecaux avait alors formé un recours pour excès de pouvoir afin de faire annuler cette délibération.

Le Conseil d'Etat s'est néanmoins prononcé sur l'anonymisation des données en affirmant que : *" (...) les procédés de " hachage " et de " salage ", s'ils visent à empêcher l'accès des tiers aux données, laissent le gestionnaire du traitement en mesure de procéder à l'identification des personnes concernées et n'interdisent ni de corréler des enregistrements relatifs à un même individu, ni d'inférer des informations le concernant"* et qu'au regard de *"l'article 2 de la loi du 6 janvier 1978, que les objectifs mêmes de la collecte des données par la société JCDecaux France étaient incompatibles avec une anonymisation des informations recueillies*"[10].

Au regard du RGPD et de cet arrêt, les transactions chiffrées effectuées dans le cadre d'une opération de trading via la blockchain pourrait donc être qualifiées d'opération non anonymes, ce qui supposerait de solliciter l'autorisation de la personne physique à qui appartiennent les données personnelles à chaque utilisation ou transfert de celle-ci sur une plateforme intermédiaire.

[10] CE, 8 fév. 2017, n° 393714

Le RGPD est-il applicable aux intermédiaires techniques de la blockchain ?

Afin de déterminer si le RGPD est applicable aux intermédiaires techniques de la blockchain, il faut établir si les intermédiaires techniques traitent des données personnelles et peuvent de ce fait être qualifiés de responsables de traitement au sens du RGPD.

Les données personnelles sont définies par l'article 4 du RGPD comme toute information permettant l'identification directe ou indirecte d'une personne physique. Ainsi, un nom, un numéro d'identification, un identifiant ou un élément spécifique à l'identité ou à la localisation d'une personne est une donnée personnelle.

Or, les éléments fournis aux intermédiaires d'achat et de revente du Bitcoin sont les données figurant notamment sur la carte d'identité ainsi que des données permettant à la plateforme de contacter l'acheteur. Ces données permettent donc d'identifier directement la personne physique qui les a soumises et répondent à la définition énoncée par le RGPD.

Ainsi les intermédiaires d'achat et de revente du Bitcoin disposent de données personnelles, mais pour pouvoir leur appliquer le RGPD, il faut qu'ils répondent à la qualification de responsable de traitement.

Le responsable de traitement est selon l'article 4 paragraphe 7 du RGPD la personne, l'autorité publique, le service ou l'organisme qui détermine les finalités et les moyens du traitement.

Le responsable de traitement peut faire appel à un sous-traitant qui agit pour son compte mais sera une entité indépendante. Dans ce cas les responsabilités du sous-traitant et du responsable de traitement pourront être mises en cause s'ils ne respectent pas leurs obligations.

L'article 4 paragraphe 2 du RGPD définit quant à lui le traitement comme toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou ensembles de données à caractère personnel. Ce traitement n'est pas forcément lié à un fichier s'il est automatisé ni ne nécessite de classement particulier.

L'article 4 paragraphe 6 du RGPD définit un fichier de données personnelles comme tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

La finalité du traitement correspond à l'objectif d'une application informatique de données personnelles selon la CNIL et doit être déclarée dans le registre de traitement prévu à l'article 30 du RGPD. Seule cette finalité devra être respectée tout au long de l'utilisation de la donnée personnelle.

Ces principes encadrent le traitement des données personnelles et sont fondamentaux pour pouvoir déterminer si le RGPD est applicable ou non.

En pratique, les plateformes d'achat et revente du Bitcoin telles que Coinbase effectuent un traitement de données personnelles puisqu'elles se chargent de les recueillir auprès de l'acheteur de Bitcoin, de les stocker et d'en transférer une partie à la plateforme de trading pour qu'elle puisse effectuer les transactions.

Les intermédiaires d'achat et revente s'occupent de stocker les données personnelles et de les transmettre aux plateformes de trading.

Ainsi, l'intermédiaire d'achat et de revente du Bitcoin semble pouvoir être qualifié de responsable de traitement au sens du RGPD ce qui devrait entrainer son applicabilité.

A l'heure actuelle, la CNIL a effectué plusieurs travaux de réflexion sur la question de la conformité de la blockchain au RGPD, mais la question des intermédiaires ne semble pas avoir été soulevée.

2. La mise en œuvre du rôle de l'intermédiaire

a) L'assurance du respect des droits des personnes concernées par le traitement

En tant que responsable de traitement, chaque intermédiaire se doit avant toute chose de s'assurer du respect des grands principes posés par le RGPD.

Le traitement est-il licite ?

Pour les intermédiaires de la blockchain Bitcoin, la licéité du traitement semble trouver son fondement dans l'article 6.1 b) du RGPD, disposant que le traitement est licite s'il est « *nécessaire à l'exécution d'un contrat auquel la personne concernée est partie…* ». En effet, la plupart des intermédiaires sont liés avec leurs utilisateurs par le biais d'un contrat d'utilisation, dont le contenu peut être disponible sur leur site internet.

Par ailleurs, l'article 6.1 c) du RGPD pourrait également trouver application. D'après cet article, le traitement peut également être licite s'il est « *nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ».* En effet, il faut noter que ces intermédiaires sont considérées comme des services de paiement, et que dès lors, ils doivent tous disposer d'un agrément de prestataire de services de paiement délivré par l'Autorité de Contrôle Prudentiel et de Résolution (ACPR). Or la délivrance de cet agrément est subordonnée au respect de certaines conditions, tenant notamment à la nécessité d'un certain contrôle interne visant à lutter, entre autres, contre le blanchiment d'argent et le financement du terrorisme. Dès lors, et comme cela est d'ailleurs indiqué sur certaines clauses de leurs contrats d'utilisation, les intermédiaires ont l'obligation de traiter des données personnelles (notamment l'identité) dans le but de répondre à ces obligations légales spécifiques.

Le traitement est-il transparent ?

C'est plus particulièrement les articles 12 et 13 du RGPD qui retiendront ici notre attention. En effet, l'article 12 dispose que le responsable du traitement doit prendre « *des mesures appropriées pour fournir toute information […] en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples…* ». L'article 13 précise quant à lui plus précisément en quoi consiste ce droit d'information lorsque des données à caractère personnel sont collectées auprès de la personne concernée.

Or, à la lecture de cette disposition, il ne semble pas évident de pouvoir conclure que le responsable de traitement soit tenu de fournir des informations relatives au fait qu'une partie des données personnelles de l'utilisateur est susceptible d'être traitée par le biais d'une application technologique, en l'occurrence la blockchain. Pourtant, son caractère de registre public invite les intermédiaires à la prudence. En effet, ne relève-t-il pas de l'obligation d'information du responsable de traitement d'avertir la personne concernée par le traitement qu'une partie de ses données personnelles est susceptible d'être accessible à tous ?

La logique inviterait à répondre par la positive, même si pour l'heure, force est de constater qu'il est loin d'être aisé de trouver trace d'une quelconque information à cet égard dans les contrats d'utilisation ou dans les informations données sur les sites de ces divers intermédiaires.

Par ailleurs, cette obligation d'information prévoit également, à l'article 13.2, a) du RGPD, que le responsable du traitement doit fournir à la personne concernée des informations sur « *la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères pour déterminer cette durée* ». En premier lieu, il se doit d'être signalé que les intermédiaires sont tout à fait à même de remplir cette obligation concernant les données personnelles directement traitées par leurs services, sans l'intervention de la blockchain.

Toutefois, la question mérite de se poser concernant l'information qu'ils se devraient de fournir à leurs utilisateurs, selon laquelle du fait de l'utilisation de la technique blockchain, une partie de leurs données personnelles serait susceptible d'être indéfiniment stockées sur un registre accessible à tous. En effet, une simple recherche sur internet permet aujourd'hui de consulter, par exemple, tous les derniers blocs de la blockchain Bitcoin[11].

Plus généralement, cette interrogation en soulève une autre d'autant plus importante, celle de l'exercice du droit à l'oubli.

L'exercice du droit à l'oubli est-il envisageable ?

Comme vu précédemment, ce droit est désormais consacré à l'article 17 du RGPD qui dispose que « *la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais* », lorsque la personne concernée peut se prévaloir de certains motifs précisément cités par cette même disposition.

Tout d'abord, il se doit d'être souligné que cette question n'a de sens que si l'on considère que les informations consultables sur le registre public de la blockchain sont effectivement des données personnelles[12]. Aux vues de ce qui a été démontré en première partie, nous partons ici du postulat que la clé publique d'un utilisateur de Bitcoin est une donnée à caractère personnel, de sorte qu'il convient donc bien de s'interroger sur la possibilité de son effacement et de son déréférencement.

Or si un premier constat mènerait à affirmer que le principe même de la blockchain empêche l'exercice de cette prérogative, le rôle de l'intermédiaire, en tant que responsable de traitement, pourrait ici s'avérer intéressant afin de résoudre une partie du problème.

---

[11] Exemple de site permettant la consultation des derniers blocs de la blockchain Bitcoin : https://blockchain.info/fr

[12] Blockchain Partner, *Blockchain et droit à l'oubli : une relation antinomique ?,* Panorama des enjeux juridiques de la Blockchain, p.13

En effet, concernant les données personnelles traitées directement par l'intermédiaire, sans l'intervention de la blockchain (c'est-à-dire le nom, le prénom, l'adresse physique et électronique, les informations bancaires…), rien n'empêche ce dernier d'effacer ces données dès lors que son utilisateur lui demande.

Ainsi, un utilisateur de Bitcoin qui souhaiterait se désinscrire d'une plateforme, et donc mettre fin à son contrat, pourrait tout à fait exiger l'effacement de ses données dans les meilleurs délais, celles-ci n'étant de fait plus nécessaires au regard des finalités pour lesquelles elles ont été collectées (article 17.1 a) du RGPD).

En revanche, reste alors la problématique de la clé publique de l'utilisateur qui serait tjs inscrite au sein du registre public de la blockchain pour toutes les transactions que ce dernier a effectué. Les données ancrées dans la blockchain étant infalsifiables, il semble ici impossible pour un utilisateur de demander l'effacement ou le déréférencement de ces informations.

Toutefois, cette énigme est à relativiser car dès lors qu'un utilisateur a exigé l'effacement des données à caractère personnel traitées par l'intermédiaire, il ne serait pas certain que les données relatives aux transactions effectuées par l'utilisateur en question, et stockées sur le registre public, permettent encore d'identifier la personne en question puisque le numéro d'identification de celui-ci (la clé publique) ne renverrait plus à une identité précise, du fait de l'effacement des données à caractère personnel par le biais de l'intermédiaire.

Il paraît toutefois important de signaler que ce droit à l'oubli serait applicable sous réserve des obligations légales spécifiques qui s'appliquent aux intermédiaires en tant que services de paiement (voir ci-dessus), qui pourraient justifier le cas échéant l'impossibilité pour l'utilisateur d'user de son droit à l'oubli sur le fondement de l'article 17.3 b) du RGPD.

b) La sécurité du traitement

Soumis au RGPD, le principe du « privacy by design » (protection des données dès la conception) s'applique également aux intermédiaires. Prévu à l'article 25 du RGPD, ce principe novateur du RGPD consiste en la mise en place de « mesures techniques et organisationnelles appropriées » compte tenu de « l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques », et ce « tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même ».

A cet égard, le règlement prend soin d'édicter de nombreuses précautions que se doit de prendre chaque responsable de traitement, telle que la désignation d'un délégué à la protection des données (article 37 du RGPD), l'incitation à élaborer des codes de conduite (article 40 du RGPD), ou encore la réalisation d'une analyse d'impact (article 35 du RGPD). Cette dernière obligation semble d'ailleurs particulièrement importante concernant les exploitants de la technologie blockchain puisque l'article 35.1 dispose que la réalisation d'une analyse d'impact par le responsable de traitement doit s'effectuer « lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, […] est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques ».

En effet, le respect de cette disposition pourrait s'avérer fondamental pour les entreprises souhaitant à l'avenir avoir recours à la blockchain qui, en tant que nouvelle technologie, pourrait en effet avoir de nombreux impacts sur les droits des personnes concernées.

Une analyse préalable de ses potentiels risques en termes de protection des données des personnes concernées par le traitement de l'entreprise en question semble donc un prérequis indispensable, et même impératif au sens du règlement.

Mais en termes de sécurité des données à proprement parler, c'est plus particulièrement le respect de l'article 32.1 du RGPD sur lequel il parait intéressant de s'attarder. Cette disposition obligent les responsables du traitement ainsi que les sous-traitant à mettre en œuvre « *les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins : la pseudonymisation et le chiffrement des données à caractère personnel… ».*

Il est donc intéressant d'analyser, dans la mesure du possible, la politique de sécurité adoptée par les divers intermédiaires eu égard à cette disposition. Or à ce titre, il convient tout d'abord de rappeler que les monnaies digitales sont par essence basées sur le chiffrement. En effet, l'un des objectifs premiers des concepteurs du Bitcoin était d'élaborer une monnaie digne de confiance, et respectueuse de la vie privée des utilisateurs. L'idée de l'invention des cryptomonnaies s'explique avant tout par le manque de confiance de ses inventeurs dans les banques suite notamment à la crise des *subprimes*, ce qui mena à l'émergence du réseau Bitcoin[13].

Ce système est basé sur le chiffrement dit asymétrique. En pratique, après avoir fourni ses données personnelles à l'intermédiaire, chaque nouvel utilisateur reçoit deux clés : une clé publique, que tout le monde connait, et qui correspond à l'adresse Bitcoin de l'utilisateur ; et une clé privée, que seul l'utilisateur connait. Sur le registre public de la blockchain, c'est cette adresse Bitcoin qui sera ancrée à chaque fois que l'utilisateur en question effectue une transaction. Or cette adresse ne permet que difficilement de remonter précisément à l'identité réelle de la personne qui se cache derrière la transaction.

En fournissant une clé publique à ses utilisateurs, chaque intermédiaire opère donc une pseudonymisation, au sens de l'article 4.5 du RGPD, qui la définit en ces termes : « *le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires* ».

[13] R. Rouphaël, *Petite histoire de la cryptographie* : BELEM, 4 janv. 2017

Toutefois, ce même article dispose également que ces informations supplémentaires « *doivent être conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable*; ».

Autrement dit, les intermédiaires doivent s'assurer, parallèlement à cette pseudonymisation, que les données personnelles fournies par les utilisateurs (nom, prénom, carte d'identité, informations bancaires, etc.) soient conservées séparément et fassent l'objet de mesures permettant d'assurer leur sécurité.

Plus généralement, un consultant en cyber sécurité nous dresse le constat suivant : « *Il est difficile d'évaluer la politique de sécurité de ces intermédiaires sans plus d'informations. Mais on peut tout de même faire deux remarques : la première est qu'aux vues de l'intérêt financier que représente les cryptomonnaies, il est clair que ces plateformes sont toutes la cible d'attaques très poussées, et qu'elles sont donc robustes. Toutefois, et encore une fois, nous n'avons que très peu d'informations à cet égard et il peut être souligné que certains d'entre eux ont fermé suite à des attaques qui ont entrainé le "vol" de nombreux bitcoins. Si ces éléments ne permettent pas un constat précis quant au niveau de sécurité des données personnelles en elles-mêmes, cela n'en reste pas moins un indicateur général de confiance.* »[14].

En résumé, il est donc difficile d'avoir d'une analyse exacte du niveau de sécurité des données personnelles traitées par les intermédiaires. Toutefois, il est clair que le principe même de la cryptomonnaie, sur lequel ils reposent, semble assurer un respect a minima des obligations auxquelles ils sont contraints.

[14] Interview réalisée avec M. Sébastien Madet, consultant en cyber sécurité chez Harmonie Technologie

Toutefois, en commentant une récente étude de l'Open Data Institute sur la blockhain, au sein de laquelle il est notamment précisé que pour protéger les données contenues à l'intérieur d'une chaine de blocs, il est nécessaire de sécuriser a minima les données via le chiffrement[15], la CNIL démontre la limite de cette solution : « Le problème de cette solution est que par principe, une blockchain est faite pour être gravée dans le marbre « pour toujours » alors que tout chiffrement court le risque d'être déchiffrable après une certaine période de temps en fonction des progrès des techniques. Si la divulgation ultérieure des données n'est pas sans conséquence, cette piste ne sera certainement pas suffisante… »[16].

Dans cette même étude, l'Open Data Institute invite également à prendre garde aux métadonnées, c'est-à-dire des données donnant des indications sur d'autres données, comme par exemple la date ou le lieu où une donnée a été produite ou enregistrée. On pourrait en effet imaginer qu'au sein d'une blockchain, des métadonnées soient inscrites dans le registre public et permettent de géolocaliser les données, créant ainsi un fort risque de réidentification de l'utilisateur concerné[17]. Un autre problème soulevé par cette institution est celui de la confiance accordée aux serveurs qui indexent le contenu de la blockchain. En effet, si le registre public de la blockchain est en lui-même infalsifiable, il convient toutefois de s'assurer de la fiabilité du moteur de recherche ou des plateformes qui mettent à disposition celui-ci auprès des utilisateurs.

En résumé, ce bref aperçu de la mise en œuvre du rôle des intermédiaires du réseau Bitcoin en tant que responsable de traitement laisse entrevoir les obligations auxquelles pourraient être soumis les futures entreprises qui souhaiteraient utiliser de nouvelles formes de blockchains publiques.

---

[15] James Smith, Jeni Tennison, Peter Wells, Jamie Fawcett, Stuart Harrison, *Applying blockchain technology in global data infrastructure*, Open Data Institute, 2016
https://theodi.org/technical-report-blockchain-technology-in-global-data-infrastructure

[16] Anuchika Stanislaus, *Les enjeux et défis des infrastructures de données utilisant la blockchain selon l'Open data institute*, Laboratoire d'innovation numérique, CNIL, 2 aout 2016
https://linc.cnil.fr/fr/les-enjeux-et-defis-des-infrastructures-de-donnees-utilisant-la-blockchain-selon-lopen-data

[17] James Smith, Jeni Tennison, Peter Wells, Jamie Fawcett, Stuart Harrison, *Applying blockchain technology in global data infrastructure*, Open Data Institute, 2016
https://theodi.org/technical-report-blockchain-technology-in-global-data-infrastructure

Et s'il ne peut aucunement être affirmé que les intermédiaires du réseau Bitcoin sont à cet égard un exemple à suivre face à l'application imminente du RGPD, force est de constater qu'ils présentent un certain nombre de garanties, notamment aux vues de leur longévité et de la relative confiance que leur accorde les utilisateurs de cryptomonnaies. Toutefois, seule la pratique pourra révéler les challenges qui attendent les futurs exploitants de nouveaux types de blockchains.

B. Les opportunités de la blockchain en tant qu'outil de protection des données personnelles

Si cette deuxième partie s'intéressait jusque-là au rôle des intermédiaires, en tant que responsables d'un traitement de données personnelles extérieurs à la technologie blockchain, il convient désormais de s'intéresser au rôle de la technologie en elle-même. Peut-elle être considérée comme un outil de protection des données personnelles ? Peut-on envisager de l'améliorer ?

1. Les avantages en termes de protection des données personnelles

Au-delà des obstacles présentés en première partie, il est clair que la technologie en elle-même présente également des avantages en termes de protection des données. Pourtant, compte tenu du fait que la création de la blockchain est intimement liée à celle du Bitcoin, et repose par ailleurs sur des mécanismes déjà existants, il n'est pas si évident de conclure en quoi cette technologie présente un caractère innovant en termes de protection des données personnelles.

En effet, il se doit d'être rappelé que « *les techniques de cryptographie sont utilisées depuis longtemps au sein des entreprises et pour les particuliers (échange de clés, connexions sécurisées, signature électroniques, certificats ...). Ces techniques n'ont pas été créées pour la cryptomonnaie. Cependant nous pouvons attribuer au Bitcoin la mise en avant de la technologie blockchain. Nous pouvons considérer que la blockchain est une nouvelle technologie, toutefois elle reste basée sur des mécanismes déjà existants (clés publiques et privées, hashage ...). »*[18].

A titre d'exemple, un premier reflex pourrait nous laisser penser que la technologie blockchain permet l'anonymat, ou du moins la pseudonymisation des données qui sont inscrites sur le registre. Nous venons en effet de démontrer, dans la sous-partie précédente, que le chiffrage asymétrique, et plus précisément la clé publique de chaque utilisateur de Bitcoin, permet la pseudonymisation lors de chacune de ses transactions. Et si c'est certes ce pseudonyme qui inscrit dans le registre public, il faut bien garder à l'esprit que le chiffrement l'ayant permis s'est opéré avant l'enregistrement de la transaction dans la blockchain.

En effet, ce sont les intermédiaires d'échanges ou de stockage de Bitcoin qui, dès qu'un utilisateur souscrit à son offre, lui donne une clé publique, et donc un pseudonyme. La pseudonymisation et le chiffrement sont donc des mesures de sécurité qui sont prises en amont par les intermédiaires, et non par la technologie blockchain en elle-même.

A cet égard, la situation nous est ainsi résumée : « *le seul et réel intérêt de la blockchain en terme de protection des données, c'est l'intégrité et la décentralisation de celles-ci. Cependant, la blockchain est aussi fiable que le nombre de ressources qui lui sont consacrées. La blockchain Bitcoin est par exemple extrêmement robuste, tandis qu'une blockchain privée avec seulement deux serveurs serait au contraire extrêmement vulnérable* »[19].

[18] Interview réalisée avec M. Sébastien Madet, consultant en cyber sécurité chez Harmonie Technologie

[19] Interview réalisée avec M. Sébastien Madet, consultant en cyber sécurité chez Harmonie Technologie

Concernant la protection des données personnelles, la distinction entre blockchain publique et privée prend en effet tout son sens. Une blockchain publique, composée d'un registre public accessible à tous, permet rappelons-le à toute personne disposant d'une capacité de calcul suffisante de pouvoir valider un bloc par la résolution d'une énigme mathématique. Fondée sur un principe de challenge, la résolution de cette énigme, qui consiste en le calcul d'un hash, permet au mineur le plus rapide de miner le block, c'est-à-dire concrètement de l'ajouter à la blockchain, à condition que la solution de l'énigme était au préalable validé par au minimum 50% des mineurs. Dès lors, plus il y a de « ressources », c'est-à-dire de mineurs susceptibles de mettre à disposition leur puissance de calculs pour résoudre le challenge mathématique, plus il y a de personnes susceptibles de valider ou non le calcul et donc l'ajout du bloc.

En résumé, plus les mineurs sont nombreux, plus l'intégrité des données contenues dans le registre est garantie. En effet, à moins de constituer plus de 51% des mineurs d'une même blockchain, ce qui est très peu probable si cette dernière est publique, il est impossible d'inscrire des données (éventuellement à caractère personnel) erronées dans son registre.

De cette manière, la blockchain publique permet de respecter l'un des principes essentiels du traitement des données à caractère personnel, à savoir l'exactitude des données qui y sont enregistrées (article 5.1, d) du RGPD).

Or, tel n'est pas le cas d'une blockchain privée. En effet, le processus d'approbation des blocks ajoutés au registre étant limités à un nombre très limités de personnes, il suffirait que ces dernières se mettent d'accord pour inscrire les informations qu'elles souhaiteraient sur le registre, sans qu'aucun tiers ne puisse vérifier la validité de cette inscription. Dès lors, une blockchain privée, à considérer qu'il s'agisse effectivement d'une blockchain, ne présente aucune réelle garantie en termes de protection des données personnelles.

Au-delà de l'intégrité des données, la blockchain a également vocation, de par son caractère décentralisé, à rééquilibrer le rapport de force entre les internautes et les tiers de confiance tels que les GAFA. En effet, comme l'explique Thibault Verbiest, Partner chez DS Avocats, la blockchain est un moyen de « redonner le pouvoir » au consommateur, en lui donnant la possibilité de décider ce qu'il partage.

Plus généralement, il ajoute que « la blockchain a en elle une promesse jusque-là non tenue par Internet, celle de l'autonomie des personnes dans leurs échanges, celle de se passer des intermédiaires, des tiers de confiance que sont les GAFA. Ces derniers ont monopolisé toute la valeur des données. »[20]. C'est en effet l'un des objectifs premiers des fervents défenseurs de la blockchain : prouver aux utilisateurs que cette technologie pourrait donner naissance à de nouveaux modèles économiques qui ne reposeraient plus sur une collecte massive de données.

2. Les perspectives d'amélioration

Victime de son succès, ou du moins de ses promesses, la blockchain fait aujourd'hui l'objet d'un grand nombre d'études visant à améliorer son fonctionnement. Si beaucoup d'entre elles vise certes à s'interroger sur les manières de la rendre toujours plus efficace et adaptée à la vie courante des affaires, il est à noter que de plus en plus de projets visent également à faire de cette technologie un réel outil de protection des données personnelles.

Beaucoup d'entre eux n'étant toutefois qu'à un stade de recherche, il est bien difficile de percevoir quels seront ceux qui auront réellement vocation à s'appliquer en pratique. Certains de ces projets retiennent toutefois déjà fortement l'attention, ne serait-ce que parce les entreprises responsables de leur développement ont signé des partenariats avec les exploitants de certaines blockchains. Tel est par exemple le cas du projet « zk-SNARK », désignant le nom d'un outil cryptographique innovant que s'apprêtent à utiliser les exploitants de la blockchain Ethereum[21].

L'idée de l'invention de ce nouvel outil est partie de la volonté de résoudre les éventuels dangers causés par la libre consultation des données sur le registre public de la blockchain. En effet, et comme cela a été vu précédemment, même si les informations sont pseudonymisées, il n'en reste pas moins qu'elles n'apportent pas une protection totale des données des utilisateurs.

---

[20] Jean-Yves Paillé, *La Blockchain redonne « le pouvoir aux patients face au GAFA », La Tribune, 12 novembre 2016*
https://www.latribune.fr/technos-medias/la-blockchain-redonne-le-pouvoir-aux-patients-face-aux-gafa-615243.html

[21] https://z.cash/fr/blog/ethereum-snarks.html

La ZCash Company a ainsi développé un outil cryptographique basé sur le principe de la preuve à divulgation nulle de connaissance. Ce principe est basé sur une volonté simple : démontrer que l'on connait un secret, sans pour autant le révéler.

Dès lors, au lieu d'avoir sur le registre public de la blockchain le pseudonyme de l'acheteur et du vendeur ainsi que le montant de la transaction, l'utilisation de cet outil cryptographique permettrait d'avoir une empreinte numérique qui serait une sorte de résultat auquel personne n'aurait pu parvenir à moins d'être le vendeur et l'acheteur en question. L'avantage est que par ce biais, le registre ne contiendrait que la preuve de l'existence de la transaction, mais pas d'informations sur cette transaction en elle-même. Pour autant, puisque les mineurs auraient la preuve que cette empreinte numérique correspond bien à une transaction, ils pourraient l'utiliser pour faire leurs calculs et vérifier que la transaction est valide[22].

L'utilisation de cet outil semble donc avoir un réel intérêt pour la blockchain, qui pourrait ainsi limiter l'insécurité de l' « *open data* » qu'elle entraîne, sans pour autant affecter son efficacité, ainsi que sa garantie d'intégrité. En effet, il serait alors possible de conclure que les données contenues au sein du registre n'auraient plus de caractère personnel, ce qui pourrait avoir pour effet de résoudre le blocage concernant l'impossibilité pour l'utilisateur d'exercer son droit à l'oubli pour les informations contenues sur le registre public de la blockchain puisque celles-ci ne seraient par nature plus compromettantes.

Plus globalement, les promesses de cette technologie blockchain nous invite à penser, de manière très prospective toutefois, que des projets futurs pourraient porter sur l'élaboration d'une blockchain dont le fonctionnement aurait pour unique objectif la protection des données personnelles des internautes.

[22] Pour une explication plus précise de l'outil : https://z.cash/technology/zksnarks.html

BIBLIOGRAPHIE

Anuchika Stanislaus, *Les enjeux et défis des infrastructures de données utilisant la blockchain selon l'Open data institute*, Laboratoire d'innovation numérique, CNIL, 2 aout 2016
https://linc.cnil.fr/fr/les-enjeux-et-defis-des-infrastructures-de-donnees-utilisant-la-blockchain-selon-lopen-data

Blockchain France, *Qu'est-ce que la blockchain ?*
https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/

Blockchain Partner, *Blockchain et droit à l'oubli : une relation antinomique ?,* Panorama des enjeux juridiques de la Blockchain, p.13

CNIL, *Comprendre les grands principes de la cryptologie et du chiffrement*, 25 octobre 2016
https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement

Dominique Legeais, Fasc. 534 : BLOCKCHAIN, JurisClasseur, 7 mars 2017

Eric A. Caprioli, *L'usine digitale : Blockchain : le délicat chemin de la confiance*, 14 novembre 216
https://www.usine-digitale.fr/article/blockchain-le-delicat-chemin-de-la-confiance.N463208

Isabelle Renard, *Régulation de la Blockchain*, 18 janvier 2017, Legalis :

Jérôme Deroulez, *Nouvelles technologies - Blockchain et données personnelles Quelle protection de la vie privée ?,* La Semaine Juridique Edition Générale n° 38, 18 Septembre 2017, 973

James Smith, Jeni Tennison, Peter Wells, Jamie Fawcett, Stuart Harrison, *Applying blockchain technology in global data infrastructure*, Open Data Institute, 2016
https://theodi.org/technical-report-blockchain-technology-in-global-data-infrastructure

Jean-Yves Paillé, *La Blockchain redonne « le pouvoir aux patients face au GAFA », La Tribune, 12 novembre 2016*
https://www.latribune.fr/technos-medias/la-blockchain-redonne-le-pouvoir-aux-patients-face-aux-gafa-615243.html

Martin-Forissier, *Blockchain et RGPD, une union impossible ?*, CNIL, Laboratoire d'innovation numérique, 24 aout 2017
https://linc.cnil.fr/fr/blockchain-et-rgpd-une-union-impossible-0

R. Rouphaël, *Petite histoire de la cryptographie* : BELEM, 4 janv. 2017
https://medium.com/belem-blockchain/4-petite-histoire-de-la-cryptographie-38d07c964f8a

Sébastien Madet, consultant en cyber sécurité chez Harmonie Technologie, entretien réalisé le 31 janvier 2018

William O'Rorke, Blockchain Partner, *Blockchain et GDPR : le malentendu*, 23 novembre 2017
https://blockchainpartner.fr/blockchain-gdpr-malentendu/