La Blockchain: comment réguler sans autorité

De Filippi, Primavera; Reymond, Michel

7

Blockchain et droit à l'oubli

Être souverain et autonome implique de ne pas dépendre d'un acteur qui a le pouvoir de couper l'accès à nos données, fermer notre compte du jour au lendemain sur un réseau social, nous empêcher de récupérer simplement nos documents… Autant de pratiques qui sont aujourd'hui très communes dans l'Internet centralisé que nous connaissons ! Mais depuis quelque temps, une alternative à ces modèles centralisés se popularise : la *blockchain*.

Si on connaît souvent la *blockchain* grâce à la monnaie numérique Bitcoin, le concept d'origine est beaucoup moins spécifique que cela. Expliquer son fonctionnement précis serait trop ardu, intéressons-nous plutôt à ses spécificités et à sa possible utilisation.

La *blockchain* est un réseau ouvert et décentralisé. Tout le monde peut la consulter. Elle vit grâce à l'activité du réseau qui l'héberge. En cas de problème avec une *blockchain*, il n'y a personne à contacter. Personne n'a le pouvoir de modifier seul la *blockchain*, ni d'en supprimer un quelconque élément. Mais son contenu est infalsifiable. Merveilleuse promesse de souveraineté ! Une communauté peut enregistrer des opérations dont elle peut garantir l'authenticité, et sans risque de laisser à une personne le pouvoir de supprimer des éléments ou la tentation de modifier l'historique à son avantage. Moins de centralisation, plus d'indépendance.

Mais la situation n'est pas aussi simple. Avoir une autorité centrale n'est pas une lubie, cela permet d'avoir quelqu'un qui garantit que les membres peuvent avoir confiance les uns dans les autres puisque quelqu'un est là pour régler les conflits et faire respecter les règles. Et si on décentralise la confiance, on décentralise également cette capacité de régler les conflits. Si demain quelqu'un enregistre sur une *blockchain* une information qui me compromet, un contenu illégal ou non libre de droit, personne n'est plus en mesure de le retirer. Pour peu que ce contenu attente à ma vie privée, c'est plutôt une impossibilité de faire respecter la souveraineté numérique des individus qui se profile. Pour illustrer cette problématique, Primavera de Filippi et Michel Reymond analysent la possibilité de faire appliquer le droit à l'oubli [1], élément emblématique de la souveraineté des individus, aux informations contenues dans une *blockchain*.

1. Le droit à l'oubli permet aux citoyens européens de demander aux moteurs de recherche le déréférencement de certaines informations les concernant.

PRIMAVERA DE FILIPPI, MICHEL REYMOND

Primavera de Filippi est chercheuse au CNRS à Paris et à l'université de Harvard. Michel Reymond est actuellement assistant post-doc à la Faculté de Droit de l'Université de Genève.

La blockchain : comment réguler sans autorité

Le 13 mai 2014, la Cour de Justice de l'Union Européenne (CJUE) rendait l'arrêt Google Spain, qui accordait aux citoyens européens le droit de demander l'effacement des résultats de recherches menant à des sites Internet contenant des informations inexactes, inadéquates ou excessives les concernant. Le droit à l'oubli repose sur le droit à la protection de la vie privée : il postule que les personnes physiques n'ont pas à rendre indéfiniment des comptes sur les événements honteux ou désagréables auxquels ils ont été associés dans un lointain passé. De façon plus large, on pourrait décrire le droit à l'oubli comme une tentative de conciliation entre, d'une part, le besoin humain d'être réhabilité ou pardonné, et, d'autre part, le rôle d'Internet en tant que registre numérique de l'histoire (Leta Jones, 2016)

Cette opposition est d'autant plus forte depuis l'apparition de nouvelles bases de données décentralisées, connues sous le nom de *blockchains*, soit la technologie utilisée par le réseau Bitcoin. Dans la mesure où la blockchain est inaltérable et résistante à la censure et à la modification par conception, elle entre en conflit direct avec le droit à l'oubli. [1] La présente contribution cherche à analyser les défis posés par ces technologies émergentes vis-à-vis du droit à l'ou-

1. Le présent article traite du droit à l'oubli tel qu'il est défini par la loi européenne, et plus précisément par la *Directive 95/46/EC du Parlement européen et du concile* du 24 octobre 1995 sur la protection des individus quant à la gestion de leurs données personnelles et de la libre circulation de ces données. Les variations légales

bli. Nous présenterons d'abord le droit à l'oubli (I) et la blockchain (II), nous analyserons ensuite si le droit à l'oubli a titre à s'appliquer à la blockchain (III) et, si tel est le cas, nous examinerons plus en avant si et comment les obligations afférant au droit à l'oubli peuvent être exécutées sur la blockchain (IV).

Définitions

Le droit à l'oubli

Le droit à l'oubli est une obligation de droit communautaire de la protection des données, imposée aux moteurs de recherche. Il permet aux citoyens européens de demander le retrait de résultats de recherches liés à leur nom et qui mèneraient à des sites Internet contenant des informations « inexactes, inadéquates ou excessives », et qui ainsi porteraient atteinte à leur vie privée. Le droit à l'oubli a été déduit par la CJUE du droit Européen de la protection des données, et notamment de la *Directive 95/46/CE*, dans l'arrêt Google Spain, en mai 2014. À l'issue de celui-ci, un ressortissant espagnol a pu amener le moteur de recherche Google à retirer un lien, apparaissant suite à une recherche portant son nom, vers une notice originellement publiée en 1998 et archivée sur le site d'un journal espagnol ; celle-ci portait sur sa participation à une vente aux enchères dans le but de recouvrer ses dettes de sécurité sociale (CJUE, 2014). L'obligation concerne tous les moteurs de recherche, mais la position hégémonique de Google sur ce marché en a fait le principal destinataire. La société a par conséquent mis en place un processus décisionnel interne pour le déréférencement et a reçu jusqu'à présent environ 500 000 requêtes, conduisant au retrait d'environ 1 500 000 résultats au total [1].

Il faut noter que le droit à l'oubli ne s'applique qu'aux liens fournis par un moteur de recherche non-spécifique à la suite de

de ce concept dans les lois nationales de certains États membres (Leta Jones, 2016) ne seront pas prises en compte ici.

1. Voir Google Inc. (28 août 2016). *Requêtes européennes de déréférencement liées à la vie privée*. Tiré de `https://www.google.com/transparencyreport/removals/europeprivacy/`.

la recherche du nom d'une personne (CJE, 2014, at par. 96). *A contrario*, il n'affecte pas directement l'intégrité du contenu référencé, comme par exemple le site web d'un journal, un article ou un billet émis sur un blog ; il n'a pas non plus vocation à s'appliquer aux résultats obtenus en cherchant des mots-clefs autres que nom et prénom. Ainsi, le droit à l'oubli est conceptuellement plus proche d'un droit limité au déréférencement plutôt qu'à un droit d'être oublié au sens littéral [1]. Et même s'il n'est pas exclu que ce droit puisse éventuellement s'appliquer au-delà des simples moteurs de recherche généralistes, et donc s'étendre à d'autre types d'intermédiaires informationnels, une telle extension nécessite que ces intermédiaires incarnent un danger similaire pour la vie privée des individus. Par exemple, cela sera le cas lorsqu'ils permettent à leur utilisateurs, lors d'une recherche portant sur un nom, d'obtenir un « aperçu structuré » leur permettant d'établir un profil plus ou moins détaillé de la personne concernée (CJUE, 2014, at pars. 37, 80 ; Article 29 DPWP, 2014, at par. 17-18).

La blockchain

Une blockchain est une base de données décentralisée qui possède quelques caractéristiques spécifiques. En premier lieu, une blockchain fonctionne comme un réseau décentralisé en pair-à-pair, qui n'est ni possédé ni contrôlé par une autorité centrale. Chaque pair du réseau possède une copie de la blockchain, et il contribue avec ses capacités de calculs à la sécurité et au maintien des opérations du réseau. En second lieu, une blockchain est une base de données à laquelle on ne peut que faire des ajouts : la seule possibilité est d'ajouter de l'information, dans l'ordre chronologique ; il est impossible de modifier ou supprimer une information une fois qu'elle est enregistrée. Enfin, une blockchain est un registre certifié [2], qui repose sur la cryptographie pour assurer que

1. La dénomination « Droit à l'oubli » est trompeuse. Une alternative appropriée serait « Droit au déréférencement ». Dans un souci de simplicité, nous utiliserons tout de même le premier.

2. Dans la mesure où une blockchain permet uniquement d'ajouter de l'information, les données ne peuvent être ni modifiées ni supprimées par qui que ce soit. On peut ainsi utiliser une blockchain pour certifier l'intégrité d'un ensemble de données

toutes les données enregistrées sont cohérentes, et ont été validées par la majorité des nœuds du réseau (Nakamoto, 2008).

Les avantages de cette technologie sont évidents, notamment sur la question de l'intégrité des données et de leur certification. Puisque personne ne peut modifier l'information stockée dans une blockchain *a posteriori*, la blockchain peut prouver qu'un document spécifique a existé, ou qu'un événement est arrivé à un moment *t* (Lemieux, 2016).

En revanche, la blockchain soulève de nombreuses inquiétudes, en majorité liées à l'inaltérabilité de l'information contenue (Vogel, 2015). La technologie fonctionne de telle manière qu'il serait impossible de supprimer du contenu illicite ou inadéquat s'il venait à être stocké dans une blockchain sans une action coordonnée de la majorité des nœuds individuels. Et dans la mesure où elles peuvent contenir des informations inadéquates, non pertinentes ou excessives, les blockchains pourraient également devenir un défi posé au droit à l'oubli. Puisqu'aucun acteur central n'est là pour contrôler le réseau, personne ne peut être tenu responsable de l'application du droit à l'oubli dans la blockchain (Umeh, 2016)

Les interactions entre la blockchain et le droit à l'oubli

L'application du droit à l'oubli à la blockchain Bitcoin

En partant des éléments expliqués ci-dessus, il pourrait être intéressant de se questionner sur l'éventuelle application du droit à l'oubli à la blockchain Bitcoin. Si, par hypothèse, un individu avait opéré une transaction gênante dans le passé, comme une inscription à un site du type Ashley Madison, pourrait-il légitimement demander la suppression de cette transaction du registre Bitcoin ?

Puisque le droit à l'oubli ne s'applique présentement qu'aux moteurs de recherche généralistes, le premier réflexe est de répondre par un « non » catégorique. On peut néanmoins se deman-

stockées à l'intérieur. De plus, toutes les données enregistrées dans une blockchain doivent être signées par la clef privée de la personne qui les ajoute. Ainsi, même si l'identité de cette personne n'est pas connue, on peut tout de même s'appuyer sur la blockchain pour certifier la source des informations contenues.

der dans quelle mesure le droit à l'oubli pourrait être étendu à la blockchain Bitcoin par analogie, la possibilité d'une telle extension n'étant, on le rappelle, non exclue d'emblée si l'intermédiaire informationnel porte un danger suffisant pour la vie privée des individus, et notamment par la diffusion d'un profil public lorsqu'on entre le nom d'une personne. Ce dernier élément de l'argument sous-tend cependant que l'exercice du droit à l'oubli exige un élément de publicité et d'accessibilité au public : c'est d'ailleurs pourquoi les moteurs de recherche ont l'obligation de prévenir à l'affichage de certains résultats mais ne sont pas pour autant amenés à retirer les liens correspondants de leur index ni à empêcher leur diffusion lors de l'emploi d'autres mots-clés que des noms (Reymond, 2016, at 41-43). Par conséquent, une personne ne devrait pas pouvoir l'invoquer pour demander la suppression d'un lien non public contenu dans une base de données en ligne ; le droit à l'oubli ne peut donc pas être invoqué pour faire supprimer certaines informations disponibles sur Internet : il ne sert qu'à protéger les citoyens de la perspective d'être indéfiniment liés à des contenus faciles à trouver sur Internet, comme dans le cas où un employeur taperait le nom de ses recrues potentielles au moment de l'embauche (Rustad & Kulevska, 2016, at 365-366).

Sur deux aspects, la blockchain Bitcoin ne répond pas à ces exigences. Premièrement, dans la mesure où le réseau Bitcoin met en relation des pseudonymes, l'information liée à la transaction notée dans le registre décentralisé ne permet pas l'identification des utilisateurs du réseau, et ne donne aucune information sur le contexte général de l'échange (De Filippi, 2016). Les individus qui font des échanges en Bitcoin ne sont désignés dans la blockchain qu'à travers leur adresse Bitcoin, un identifiant global sous forme d'une chaîne de caractères de ce type : 37WctrDb1G1orXhJ8vgx7zS2WCuSuBk6EQ. Aucune autre information n'est disponible, ni sur leur identité hors ligne, ni sur la nature de leur transaction. Ainsi, les informations stockées dans la blockchain Bitcoin ne pose pas d'effet visible sur la vie privée des personnes qu'elle répertorie, ou en tout cas dans aucune mesure comparable à un moteur de recherche. Deuxièmement, les infor-

mations stockées sur la blockchain ne sont pas accessibles librement, ou tout du moins avec bien moins d'aisance qu'avec un site web ou un moteur de recherche. De par sa nature en tant que base de données décentralisée distribuée sur un réseau d'ordinateurs, la blockchain Bitcoin n'est véritablement accessible qu'aux seuls utilisateurs ayant les moyens logistiques et informationnels leur permettant d'installer les logiciels nécessaires pour obtenir l'accès au réseau et à en miner les données contenues. Évidemment, cette tâche requiert une connaissance et des efforts incomparables à ceux fournis pour consulter un site Internet.

Bien entendu, nous n'entendons pas par là que le droit à l'oubli ne peut pas s'appliquer aux intermédiaires qui fournissent une interface permettant de consulter directement la blockchain Bitcoin. Le site Internet blockchain.info, par exemple, fournit un accès simple et mis à jour en temps réel sur l'état du registre Bitcoin, quoiqu'il ne lie aucune donnée de transaction à des informations qui permettraient d'identifier des personnes.

À l'inverse, si le site Internet permettait de lier des adresses Bitcoin à des noms et prénoms réels, et de permettre la recherche d'entrées par noms dans ce cadre, nous aurions potentiellement un cas d'application du droit à l'oubli. Cependant, même dans ce cas, l'obligation de déréférencement ne s'appliquerait qu'à ce site en particulier, et uniquement en vertu de sa fonction de portail direct de recherche dans la blockchain Bitcoin. Le droit à l'oubli ne concernerait donc en aucun cas la blockchain Bitcoin en tant que telle.

Le droit à l'oubli appliqué à d'autres usages de la blockchain (le cas Steem.it)

La blockchain Bitcoin n'est qu'un exemple parmi tant d'autres des usages possibles de cette technologie émergente. À la suite de la popularisation du Bitcoin, de nombreuses autres applications basées sur la blockchain ont été développées, chacune avec leurs caractéristiques propres (Crosby & al., 2016). Pour le moment, la plupart d'entre elles relèvent du domaine de finance, mais quelques unes apparaissent dans le domaine de la création et de la distribution de contenu (Swan, 2015). Steem.it est un exemple emblema-

tique de cette tendance ; il s'agit une plateforme de publication et de réseau social basée sur la blockchain dont le principe tient à la favorisation et à la rémunération, à l'aide d'une monnaie virtuelle, des contributions de ses utilisateurs. Ces contributions peuvent prendre plusieurs formes, allant de la publication de contenu original (des billets de blog, des vidéos, des images, etc.) à la conservation active de la plate-forme par l'appréciation du contenu soumis par d'autres utilisateurs (commentaire, votes positifs et négatifs…)

Steem.it est basé sur sa propre blockchain, dans laquelle chaque contribution est stockée grâce aux métadonnées appropriées (identité du contributeur, commentaires, votes reçus). Le contenu textuel est directement stocké dans la blockchain, et les images et vidéos sont hébergées par des solutions tierces : seul le lien vers ce contenu est stocké dans la blockchain. On pourrait affirmer que la blockchain Steem.it pourrait être concernée par le droit à l'oubli, au moins dans la mesure où certains pourraient l'utiliser pour extraire des informations liées à des individus spécifiques.

Cependant, comme décrit ci-dessus, le contenu enregistré dans une blockchain ne peut plus être ni modifié, ni supprimé par qui que ce soit dans la mesure où la technologie de la blockchain est, par essence, inaltérable. Ainsi, l'intégralité du contenu enregistré dans la blockchain Steem.it est impossible à censurer. Et puisqu'il n'y a aucune autorité centrale qui gère le réseau, aucun gouvernement ne peut adresser de requête visant la suppression d'informations sensibles ou de contenu considéré comme illicite.

Cela étant, la plupart des utilisateurs de Steem.it n'interagissent pas directement avec sa blockchain, mais se contentent d'accéder aux contenus via son site Internet, qui est, lui, géré de manière centralisée. En effet, le site Internet de Steem.it collecte des informations sur les contributions de la blockchain Steem.it, et les présente de manière claire et accessible, avec le nom des contributeurs. Tous les contenus ne sont pas affichés sur le site : à la suite de l'évaluation de ces contenus, ceux qui ont reçu des votes négatifs finissent par disparaître du site – quoiqu'ils restent stockés dans la blockchain. En ce sens, le site Internet de Steem.it peut être considéré comme un intermédiaire (ou plutôt un infomédiaire) qui collecte

les informations d'une base de données et les rend accessibles au public en fonction de critères spécifiques. En tant que tel, on pourrait tout à fait invoquer le droit à l'oubli pour demander aux administrateurs du site Internet de Steem.it de retirer un contenu qui divulguerait des informations inadéquates ou excessives sur une personne.

L'application du droit à l'oubli pourrait cependant être difficile dans la mesure où le site de Steem.it, tout centralisé qu'il soit, manque d'une structure centralisée de modération et d'administration. La modération est effectuée par les utilisateurs eux-mêmes, qui prennent la responsabilité de donner des votes négatifs aux contenus qu'ils considèrent comme inappropriés. Autoriser la suppression d'un contenu qui n'aurait pas reçu de votes négatifs de la part de la communauté de Steem.it contreviendrait à leur politique et pourrait dissuader leurs utilisateurs de continuer à utiliser le site Internet. De plus, dans la mesure où toutes les informations de la blockchain de Steem.it sont publiques, il est impossible d'empêcher des tiers de développer leurs propres versions alternatives (de type darknet) du site de Steem.it et de proposer un accès exhaustif à la blockchain, y compris aux informations indésirables, à ceux qui voudraient réellement y avoir accès.

L'exécution du droit à l'oubli sur la blockchain

Problématiques

Imaginons une plateforme fictive basée sur la blockchain qui fonctionnerait comme un LinkedIn décentralisé, nourri par les contributions de ses utilisateurs. Cette blockchain serait un registre dans lequel n'importe qui pourrait ajouter des informations au sujet d'une personne en particulier – par exemple, en fournissant des liens vers un contenu déjà disponible sur Internet. Toute personne qui souhaiterait en savoir plus sur un individu pourrait parcourir le contenu accumulé par l'entier des utilisateurs. Dans un tel scénario, il va sans dire que le droit à l'oubli pourrait légitimement être invoqué, car ce service permettrait à n'importe qui d'accéder à une sorte de profil public de la personne, qui pourrait inclure des liens

ou des références à des informations « inexactes, inadéquates ou excessives ». Certes, on pourrait argumenter que l'élément de publicité n'est pas rempli, car ces informations seraient moins immédiatement consultables que si elle étaient indexées par un moteur de recherche ou même disponibles sur le véritable LinkedIn, mais dans l'hypothèse où la blockchain serait accessible à n'importe qui, il reste vraisemblable que le droit à l'oubli puisse être invoqué pour demander la suppression de certains liens et contenus.

L'application hypothétique du droit à l'oubli à une telle plateforme soulève de nombreuses interrogations quant au degré de responsabilité des acteurs qui la font vivre, ainsi qu'à leurs devoirs. Contrairement aux plateformes traditionnelles qui fonctionnent sur un modèle centralisé et dont on peut facilement identifier le fournisseur d'accès, un réseau blockchain est opéré par chacun des nœuds du réseau, de manière décentralisée – il n'existe aucune entité centrale ayant l'autorité ou la capacité technique d'ajouter, supprimer ou modifier les informations stockées dans la blockchain.

Ainsi, on peut légitimement se demander comment un LinkedIn décentralisé pourrait appliquer le droit à l'oubli dans le cas où un citoyen européen demanderait la suppression d'un lien contenu dans la blockchain. En l'absence d'intermédiaire, qui serait responsable d'assurer la mise en œuvre de cette requête ? Et qui serait tenu, le cas échéant, responsable d'un tel manquement au droit à l'oubli ?

À première vue, dans la mesure où la blockchain est par essence inaltérable et que le stockage d'informations est irréversible, demander la suppression d'un élément de la blockchain semble tout simplement absurde, puisqu'impossible à réaliser techniquement. Et puisque personne n'a le pouvoir de supprimer unilatéralement les données d'une blockchain, personne ne peut être tenu responsable de la non-suppression de certaines informations.

Cependant, résumer ainsi les liens entre blockchain et droit à l'oubli est assez réducteur. De fait, l'action coordonnée des nœuds actifs du réseau permet de supprimer certaines données d'une blockchain. Dans le cas du Bitcoin, par exemple, deux transactions apparemment valides mais incompatibles l'une avec l'autre

(l'exemple classique est une double dépense des mêmes fonds de départ) seront sujettes au protocole de consensus décentralisé de Bitcoin, qui permettra de décider de la transaction à conserver et de celle qu'il faut supprimer (Nakamoto, 2008) – alors que cela implique clairement de changer l'état actuel de la blockchain. On pourrait imaginer que cette technique s'applique au retrait de contenu illégal (contenus sous copyright, discours d'incitation à la haine ou pédopornographie) d'une blockchain publique. S'il y a consensus sur le fait que certains contenus soient inappropriés vis-à-vis de la plateforme, il est techniquement possible de les retirer de la blockchain. Bien entendu, c'est trouver ce consensus au sein d'un réseau décentralisé qui pose la principale difficulté (De Filippi & Loveluck, 2016), et ne pas y parvenir a parfois des conséquences inattendues.

Ethereum et ses implications sur le droit à l'oubli

L'exemple récent du *hack* de *TheDAO* nous fournit une bonne illustration de ces différentes problématiques : à la suite de ce *hack*, la blockchain Ethereum s'est séparée en deux réseaux différents : Ethereum et Ethereum Classic. Cet événement n'impliquait certes aucune question de vie privée ou de liberté d'expression, mais son analyse permet d'avoir un aperçu pertinent des enjeux du caractère inaltérable de la blockchain.

Ethereum est une plateforme blockchain de cryptomonnaie semblable au Bitcoin. Lancée en juin 2015, elle permet à ses utilisateurs d'échanger des jetons Ether (ou ETH). Contrairement au Bitcoin, la blockchain Ethereum inclut un langage Turing-complet, qu'on peut utiliser pour inclure du logiciel dans ses transactions. Pour donner un exemple concret : Alice pourrait vouloir mettre en place un versement régulier à Bob à chaque fois qu'un événement spécifique survient. En intégrant ces instructions à la blockchain, le paiement sera effectué comme prévu, sans qu'Alice ni Bob n'aient besoin de faire quoi que ce soit de leur côté. Ces possibilités, qui existent sous la dénomination de contrats intelligents, peuvent concerner des conditions très simples ou des montages logiciels très complexes.

Dans ce contexte, *TheDAO* (abréviation de Organisation Autonome Décentralisée) a été lancé en avril 2016. L'objectif de *TheDAO* était de mettre en place une organisation complètement automatisée, dont les règles de fonctionnement s'appliquaient dans le cadre des contrats intelligents. Le code permettait à des investisseurs d'envoyer des fonds dans un portefeuille commun, et de recevoir un nombre de jetons proportionnel à leur investissement, ce qui leur permettait de participer à la gouvernance et à la prise de décisions de l'organisation en question. Un mois après son lancement, l'organisation avait déjà attiré 150 millions d'Ether d'investissement. Un tiers de la valeur de l'argent investi fut dérobé le 18 juin 2016 par un attaquant non-identifié [1] qui avait exploité une vulnérabilité dans le code des contrats intelligents.

Devant l'indignation provoquée par cet événement, la communauté Ethereum a décidé d'intervenir en mettant en place une action coordonnée pour effectuer des modifications dans la blockchain Ethereum (un *hard fork*). Tous les participants actifs du réseau ont été invités à passer à une version alternative du registre, dans lequel les fonds qui avaient été volés n'appartenait plus à l'attaquant mais étaient déposés dans un compte créé pour l'occasion pour que les investisseurs récupèrent leur argent. Cette solution n'a pas fait l'unanimité : quelques utilisateurs ont avancé que cette action compromettait l'inaltérabilité de la blockchain et ont refusé d'adopter cette version alternative. Cet événement a conduit à l'émergence d'une blockchain Ethereum alternative – Ethereum Classic – qui rejetait le *hard fork* et conservait la blockchain originale.

Il y a de nombreux enseignements à tirer de cette histoire. Avant tout, elle donne la preuve que les blockchains peuvent être modifiées. Si elle se retrouve face à des sanctions économiques ou juridiques, la communauté qui fait vivre une blockchain peut prendre la décision d'intervenir collectivement pour censurer une transac-

1. Dans la mesure où il n'y a eu ni intrusion ni effraction dans le système, on peut se demander si les fonds en question ont effectivement été « volés » par un « attaquant » ou s'ils ont simplement été récupérés par un individu très bon techniquement qui a réussi à comprendre comme utiliser le code à son avantage pour transférer l'argent à une tierce partie.

tion spécifique ou supprimer des informations y contenues. Mais la nécessité de respecter les lois européennes de protection des données seront-elles une incitation suffisante ? La question reste ouverte. Le second enseignement à tirer de l'exemple d'Ethereum est le constat que même si la majorité de la communauté souhaite collaborer avec les autorités chargées de faire respecter la loi, il est difficile de faire disparaître les informations de la blockchain sans le consensus de toute la communauté. Il suffit d'un simple désaccord pour que la blockchain se sépare en deux réseaux différents.

Conclusion

L'apparition de la blockchain va avoir d'indéniables conséquences sur la régulation de la mise à disposition des informations, notamment d'un point de vue technique : les données d'une blockchain ne peuvent être modifiées ni supprimées. Il est cependant plus difficile d'évaluer l'impact de l'émergence de ces nouvelles technologies sur la possibilité de faire appel au droit à l'oubli. De fait, ce n'est pas la résistance à la censure de la blockchain qui pose directement problème : le droit à l'oubli ne peut pas, du moins dans sa version actuelle [1], donner lieu à une demande de suppression de contenu, mais uniquement le déréférencement de ce contenu. Bien entendu, il n'est pas exclu que des citoyens européens puissent légitimement invoquer le droit à l'oubli dans le cas où des liens de ce type seraient stockés dans une blockchain et où ils permettraient à un large groupe d'utilisateurs d'accéder à des informations inexactes, inadéquates ou excessives. Dans ce cas précis, les spécificités techniques de la blockchain risqueraient de poser problème à l'application du droit à l'oubli. Dans la mesure où la blockchain n'est pas gérée par un administrateur central, au-

1. L'avenir du droit à l'oubli est à examiner au regard du passage en force, dans moins de deux ans, du Règlement général européen sur la protection des données (GDPR), qui contient notamment un « droit à l'oubli » dans son article 17. On ne sait pas encore si ce droit à l'oubli se contente de réaffirmer ce qui se fait aujourd'hui sous l'arrêt Google Spain ou s'il contient de nouveaux aspects (*Contrast Rustad & Kulevska*, 2016, at 367-370. Voir aussi Daphne Keller « The Final Draft of Europe's Right to be Forgotten Law », *Center for Internet and Society*, 17 déc. 2015, cyberlaw.stanford.edu.

cune entité n'a l'autorité ni la capacité de modifier ou supprimer unilatéralement des éléments de la blockchain. La seule possibilité de modifier ou supprimer les données incriminées implique un accord et une action coordonnée de l'intégralité – ou au moins d'une large majorité – des nœuds actifs d'une blockchain, qui effectuerait de manière cohérente les modifications nécessaires (Wright & De Filippi, 2015). Bien entendu, l'exemple d'Ethereum nous a montré que même s'il existait un large consensus autour d'une modification de la blockchain, il suffit d'une petite minorité qui rejette la modification pour qu'elle puisse maintenir une version non-modifiée de la blockchain.

Bibliographie

Article 29 Data Protection Working Party, November 26, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on « Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzàlez », C-131/12, 14/EN, WP 225.

CROSBY Michael et *al.*, « BlockChain Technology : Beyond Bitcoin », in *Applied Innovation Review*, **2**, 2016. http://scet.berkeley.edu.

DE FILIPPI Primavera, « The interplay between decentralization and privacy : the case of blockchain technologies », in *Journal of Peer Production*, **9**, 2016. http://peerproduction.net/.

DE FILIPPI Primavera et Benjamin LOVELUCK « The invisible politics of Bitcoin : governance crisis of a decentralized infrastructure », *Internet Policy Review*, **5**(4), 2016. `http://policyreview.info`.

European Court of Justice, May 13 2014, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12.*

LEMIEUX Victoria, « Trusting Records : Is Blockchain Technology the Answer ? », *Records Management Journal*, **26**(2), 2016, p. 110-139. http://www.emeraldinsight.com.

LETA JONES Meg, *Ctrl+Z : The Right to be Forgotten*, New York, NY : New York University Press, 2016.

NAKAMOTO Satoshi, « Bitcoin : A peer-to-peer electronic cash system », *bitcoin.org*. https://bitcoin.org/bitcoin.pdf.

REYMOND Michel Jose, « Hammering Square Pegs into Round Holes : The Geographical Scope of Application of the EU Right to be Delisted », *Berkman Klein Center Research Publication*, **12**, 2016. http://ssrn.com/abstract=2838872.

RUSTAD Michael L. et Kulevska Sanna, « Reconceptualizing the Right to be Forgotten to Enable Transatlantic Data Flow », *Harvard Journal of Law & Technology*, **28**(2), 2015, 349-417. http://ssrn.com/abstract=2627383.

SWAN Melanie, *Blockchain : Blueprint for a new economy*, Sebastopol, CA : O'Reilly Media, Inc., 2015.

UMEH Jude, « Blockchain Double Bubble or Double Trouble ? », *ITNOW*, **58**(1), 2016, p. 58-61. http://itnow.oxfordjournals.org/content/58/1/58.abstract

VOGEL Nick, « The Great Decentralization : How Web 3.0 Will Weaken Copyrights, 15 J. Marshall Rev. Intell. Prop. L. 136 », in *The John Marshall Review of Intellectual Property Law*, **15**(1), 2015, p. 137-149. http://repository.jmls.edu/ripl/vol15/iss1/6.

WRIGHT Aaron et DE FILIPPI Primavera, « Decentralized blockchain technology and the rise of lex cryptographia », à paraître. http://ssrn.com/abstract=2580664