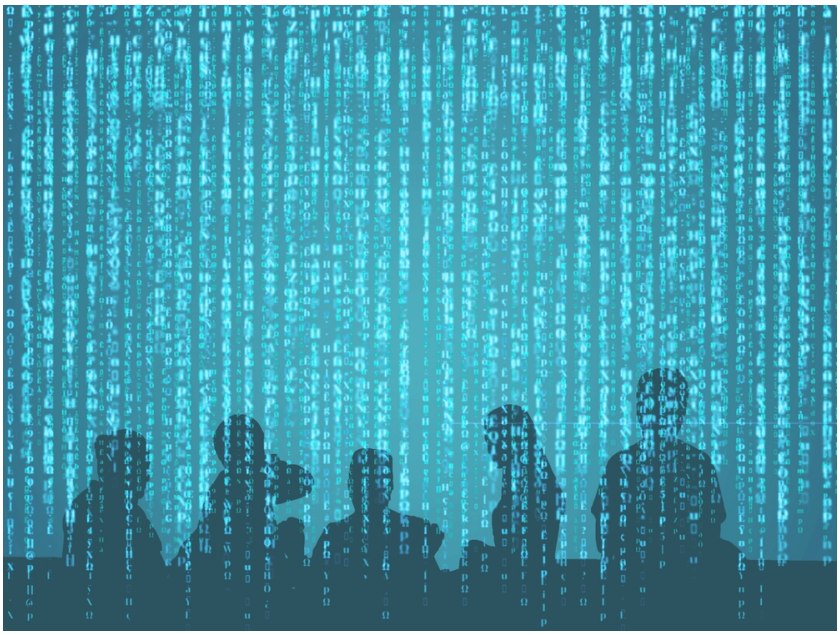
Parlement européen

Comment la technologie de la chaîne de blocs pourrait changer nos vies



ANALYSE APPROFONDIE

EPRS | Service de recherche du Parlement européen
Auteur: Philip Boucher
Unité de la prospective scientifique (STOA)
PE 581.948

FR

.

Comment la technologie de la chaîne de blocs pourrait changer nos vies

Analyse approfondie

Février 2017

PE 581.948

AUTEURS

Philip Boucher,	Unité de la prospective scientifique (STOA), DG EPRS, Parlement Européen
Susana Nascimento,	Unité de la prospective, des études comportementales et de la conception des politiques, DG JRC, Commission Européenne (parties 6 à 8)
Mihalis Kritikos,	Unité de la prospective scientifique (STOA), DG EPRS, Parlement Européen (parties sur l'élaboration de politiques d'anticipation)

VERSIONS LINGUISTIQUES

Original: EN
DE, ES, FR, IT, PL, PT

À PROPOS DE L'ÉDITEUR

Pour contacter la STOA ou pour vous abonner à sa lettre d'information, veuillez écrire à l'adresse suivante: STOA@ep.europa.eu
Ce document est disponible sur Internet à l'adresse suivante: http://www.ep.europa.eu/stoa/

Rédaction achevée en février 2017

CLAUSE DE NON-RESPONSABILITÉ

PE 581.948
ISBN 978-92-846-1043-3
doi: 10.2861/722047
QA-02-17-043-FR-N

Sommaire

Comment la technologie de la chaîne de blocs pourrait changer nos vies

Les chaînes de blocs constituent un moyen remarquable de tenir un registre de transactions de manière transparente et décentralisée. Elles sont surtout connues pour être à la base de devises numériques comme le bitcoin, qui a mis la technologie de la chaîne de blocs sous le feu des projecteurs lorsqu'il s'est apprécié de 1 000 % en l'espace d'un seul mois en 2013. Cette bulle avait alors éclaté rapidement, mais le bitcoin connaît une croissance régulière depuis 2015 et son cours atteint aujourd'hui un niveau plus élevé que jamais.

Il existe de nombreuses manières de créer de nouvelles monnaies à l'aide des chaînes de blocs. Des centaines de ces monnaies ont été conçues avec des caractéristiques et des objectifs propres. Comme les transactions de devises fondées sur les chaînes de blocs génèrent des registres publics sûrs, rapidement et à moindre coût, elles pourraient servir à de nombreuses fins non financières, par exemple pour voter à une élection ou prouver qu'un document existait à une date précise. Les chaînes de blocs conviennent tout particulièrement dans les situations où il est nécessaire de conserver un historique de propriété. Ainsi, elles pourraient faciliter la gestion des chaînes d'approvisionnement, en vue de s'assurer que des diamants sont de provenance éthique, que des vêtements n'ont pas été fabriqués dans un atelier clandestin ou que le champagne vient bien de Champagne. Elles pourraient permettre de résoudre enfin le problème du piratage de la musique et des films, en offrant la possibilité d'acheter, de vendre, d'hériter ou de céder en toute légitimité des contenus numériques à l'instar des livres, des disques et des cassettes vidéo. Elles ouvrent également des possibilités dans toutes sortes de services publics, comme le remboursement des frais de santé et le versement des prestations sociales. À la pointe du développement des chaînes de blocs se trouvent même les contrats intelligents, qui laissent entrevoir un avenir où des entreprises autonomes fonctionneraient sans intervention humaine.

Les chaînes de blocs redistribuent aux utilisateurs une partie du contrôle qu'exercent les élites centralisées sur les interactions technologiques du quotidien. Elles rendent ainsi les systèmes plus transparents, voire plus démocratiques. Pour autant, cela n'aboutira probablement pas à une révolution. En effet, les États et les géants du secteur qui investissent massivement dans la recherche et développement en matière de chaînes de blocs n'ont pas pour objectif de se rendre eux-mêmes obsolètes, mais plutôt d'améliorer leurs services. La problématique est d'ailleurs plus vaste. Par exemple, la transparence des chaînes de blocs convient bien aux registres publics tels que les cadastres, mais qu'en est-il des comptes bancaires et autres données sensibles? Il est possible, quoique seulement parfois et au prix d'efforts substantiels, d'identifier les personnes associées aux transactions. Cela pourrait compromettre leur vie privée et leur anonymat. Si certaines chaînes garantissent bien un anonymat total, certaines informations sensibles ne doivent tout simplement pas être distribuées de la sorte. Néanmoins, même si les chaînes de blocs ne sont pas la solution à tous les problèmes et ne révolutionneront pas tous les aspects de nos vies, elles pourraient avoir des répercussions importantes dans de nombreux domaines, et il est nécessaire d'être préparé aux défis qu'elles présentent et aux possibilités qu'elles offrent.

La présente analyse informe, de manière accessible, celles et ceux, au Parlement européen et ailleurs, qui souhaitent en savoir plus sur le développement des chaînes de blocs et leurs retombées potentielles. Cette démarche a pour objectif de stimuler la réflexion et les discussions autour de cette technologie complexe, controversée et à l'évolution rapide. L'analyse n'est pas séquentielle, ainsi le lecteur est-il invité à choisir les parties qui l'intéressent et à les lire dans l'ordre de son choix. La première partie présente un aperçu du mode de fonctionnement de la technologie de la chaîne de blocs. Les huit parties suivantes détaillent chacune sur deux pages les applications possibles de cette technologie dans des domaines variés, les incidences potentielles et les enjeux en matière de politique européenne. Enfin, la conclusion formule quelques remarques générales et offre plusieurs réponses possibles au développement des chaînes de blocs.

Comment les chaînes de blocs fonctionnent-elles?

Avant de chercher à comprendre comment fonctionnent les registres reposant sur des chaînes de blocs, il est utile de se pencher sur les registres traditionnels. Depuis des siècles, les banques ont recours à des livres comptables pour tenir les écritures des transactions, et les États utilisent des cadastres pour enregistrer la propriété foncière. Une autorité centrale, la banque ou une agence de l'État, est chargée de gérer les modifications au registre des transactions, ce qui lui permet d'identifier le détenteur d'une propriété donnée à tout moment. Elle peut ainsi vérifier si une nouvelle transaction est légitime, si les mêmes 5 euros ne sont pas dépensés deux fois et si des maisons ne sont pas vendues par des personnes qui ne les possèdent pas. Étant donné que les utilisateurs comptent sur le gestionnaire du registre pour vérifier la validité des transactions, ils peuvent acheter et vendre des biens entre eux, et ce, même s'ils ne se sont jamais rencontrés auparavant et qu'ils ne se font pas confiance. L'intermédiaire contrôle également l'accès aux informations contenues dans le registre. Il peut ainsi décider que tout un chacun peut connaître l'identité du propriétaire d'un immeuble, mais que seul le titulaire d'un compte peut en vérifier le solde. Ces registres sont **centralisés** (ils reposent sur un intermédiaire, auquel tous les utilisateurs font confiance, qui exerce un contrôle total sur le système et qui supervise chacune des transactions) et sont des **boîtes noires** (leur fonctionnement ainsi que leurs données ne sont pas entièrement visibles par l'utilisateur). La numérisation a rendu ces registres plus rapides et d'utilisation plus aisée, mais ils demeurent centralisés et opaques.

Les chaînes de blocs offrent la même fonctionnalité de tenue de registres, mais sans architecture centralisée. Quelle est alors la légitimité d'une transaction s'il n'existe pas d'autorité centrale à même de la vérifier? Les chaînes de blocs résolvent ce problème en décentralisant le registre, de sorte que chaque utilisateur en détienne une copie. N'importe qui peut demander l'ajout d'une transaction à la chaîne de blocs, mais une transaction n'est acceptée que si l'ensemble des utilisateurs s'accordent sur sa légitimité, par exemple sur le fait que la demande provient bien d'une personne habilitée, que le vendeur de la maison ne l'a pas déjà vendue, et que l'acheteur n'a pas déjà dépensé l'argent. Cette vérification s'effectue de manière fiable et automatique pour le compte de chaque utilisateur, ce qui crée un système de registre très rapide, sûr et remarquablement résistant à la falsification.

Chaque nouvelle transaction à enregistrer est assemblée avec toutes les autres transactions récentes dans un «bloc», qui devient le dernier maillon de la longue «chaîne» de l'historique des transactions. Cette chaîne de blocs constitue le registre qui est détenu par tous les utilisateurs. Cette opération est appelée «minage». Tout le monde peut devenir un mineur et tenter d'être le premier à résoudre le problème mathématique complexe qui consiste à créer un bloc de transactions valide et chiffré en vue de l'ajouter à la chaîne de blocs. Il existe divers moyens d'inciter les gens à effectuer ce travail. Le plus souvent, le premier mineur qui crée un bloc valide et l'ajoute à la chaîne est récompensé par la somme des commissions sur les transactions contenues dans ce bloc. Ces commissions s'élèvent actuellement à environ 10 centimes d'euro par transaction, mais des blocs sont ajoutés régulièrement et contiennent des milliers de transactions. Les mineurs peuvent également recevoir de nouvelles devises, créées et mises en circulation au titre d'un mécanisme inflationniste.

L'ajout d'un nouveau bloc à la chaîne suppose la mise à jour du registre détenu par l'ensemble des utilisateurs. Les utilisateurs n'acceptent un nouveau bloc que lorsqu'il a été vérifié que toutes ses transactions sont valides. Si une anomalie est décelée, le bloc est alors rejeté. Autrement, le bloc est ajouté et conservera sa position en tant que registre public. Aucun utilisateur ne peut l'effacer. Si une attaque contre l'intermédiaire suffit pour détruire ou altérer un registre traditionnel, il est nécessaire, dans le cas d'une chaîne de blocs, de réussir une attaque simultanée contre chacune des copies du registre. Il ne peut exister de faux registre, car tous les utilisateurs disposent de leur propre version authentique pour le vérifier. La confiance et le contrôle des transactions fondées sur les chaînes de blocs ne sont pas centralisés et opaques, mais **décentralisés** et **transparents**. Ces chaînes de blocs sont décrites comme étant «sans permissions», car il n'existe pas d'autorité spéciale pouvant refuser la permission de

participer à la vérification et à l'ajout des transactions. Elles peuvent aussi être considérées comme l'incarnation de valeurs politiques et sociales, comme la transparence et la redistribution du pouvoir.

Il est également possible de mettre en place des chaînes de blocs «à permissions», pour lesquelles un groupe limité d'acteurs conserve la faculté d'accéder au registre, de le vérifier et d'y ajouter des transactions. Cela permet aux acteurs «institutionnels», tels que les banques et les États, de garder un grand contrôle sur leurs chaînes de blocs. Les chaînes de blocs à permissions sont moins transparentes et décentralisées que leurs homologues sans permissions, si bien qu'elles incarnent des valeurs sociales et politiques légèrement différentes.

1. Devises: l'avant-garde de la technologie de la chaîne de blocs

Les devises constituent de loin la plus célèbre des nombreuses utilisations de la technologie de la chaîne de blocs. De même, alors que le bitcoin n'est que l'une des multiples monnaies créées d'après ce principe, c'est de loin la plus connue. De nombreux projets récents ont porté sur les vastes possibilités offertes par cette technologie, mais il est rare qu'un débat public sur les chaînes de blocs ne fasse pas référence au bitcoin ou, du moins, aux devises fondées sur les chaînes de blocs. Étant donné que les monnaies dominent le débat autour des chaînes de blocs et qu'elles en représentent l'application la plus mûre et la plus connue, elles exercent une profonde influence sur le développement de cette technologie à titre plus général. Cette partie offre un bref aperçu du fonctionnement des applications de chaînes de blocs pour les monnaies et quelques-unes de leurs incidences. Toutefois, comme il existe déjà plusieurs guides et articles disponibles sur le sujet, l'importance sera accordée à la manière dont la prépondérance du bitcoin dans le domaine des chaînes de blocs est susceptible d'influencer le développement général de la technologie et les autres applications des registres distribués.

Comment ces devises fonctionnent-elles?

Le bitcoin a été lancé par Satoshi Nakamoto, pseudonyme utilisé par un ou plusieurs mystérieux auteurs d'un article qui décrit comment la cryptographie, associée à un registre public distribué, pourrait servir à créer une devise numérique libérée de toute autorité centralisée de vérification des paiements. Habituellement, un individu peut échanger de l'argent avec une personne qu'il ne connaît pas car les deux acteurs ont confiance en une tierce partie, que ce soit en la validité d'un billet de banque ou en un intermédiaire comme une banque ou un bureau de change. Le système imaginé par Nakamoto ne comporte ni monnaie fiduciaire ni intermédiaire, mais instaure un climat de confiance grâce à l'utilisation innovante de la cryptographie et des réseaux de pair à pair. Lorsqu'un utilisateur envoie des bitcoins à un autre, les détails de la transaction, tels que les adresses des deux parties et le montant transmis, sont diffusés sur le réseau bitcoin afin d'être validés par tous les pairs du réseau. Une fois validée par le réseau, la transaction est incluse dans un «bloc» de transactions et ajoutée, au moyen du processus de «minage», à la liste toujours croissante des blocs qui composent le registre de la chaîne de blocs. Cette liste est enregistrée par l'ensemble des pairs présents sur le réseau. Le bitcoin dispose également d'une fonction qui génère de nouveaux bitcoins et les injecte dans le système, avec pour résultat de créer de l'inflation. Ces bitcoins sont distribués aux mineurs (en plus de la somme des commissions des transactions dans le bloc) en tant que récompense pour l'ajout de transactions à la chaîne de blocs. N'importe quel utilisateur peut entreprendre de miner à l'aide de son ordinateur, mais les mineurs se sont professionnalisés et utilisent aujourd'hui des ordinateurs spécialement conçus pour cette tâche. La structure répartie du système, alliée à sa fonctionnalité cryptographique, rendent le bitcoin incroyablement robuste. La confiance nécessaire pour effectuer des transactions est établie par le fait que toutes les transactions, d'hier, d'aujourd'hui et de demain, sont observées, quoique de manière automatique, par tous les utilisateurs.

Le bitcoin est de loin la principale devise fondée sur les chaînes de blocs, mais il en existe de nombreuses autres qui présentent de légères différences techniques. Ces différences résident souvent dans le

processus de minage, qui peut demander d'importantes ressources de calcul. Par exemple, certaines monnaies reposent sur des algorithmes moins gourmands en ressources que le bitcoin. L'algorithme du peercoin est ainsi conçu pour utiliser de moins en moins de ressources au fur et à mesure qu'il se développe. Ces devises varient également sur le plan du rythme et des modes de création et de distribution de nouvelle monnaie, c'est-à-dire sur le plan de leur politique d'inflation. Beaucoup définissent un nombre maximum de «coins», et, dès lors que cette valeur est atteinte, le minage ne crée plus de nouvelle monnaie et les mineurs tirent seulement profit des commissions sur les transactions. Certaines devises reposent sur des algorithmes conçus pour éviter l'apparition de mineurs professionnels qui utilisent un équipement de minage spécialisé.

Comme ces transactions ont un coût très faible, qui se situe aujourd'hui entre 0 et 0,10 euro, mais qu'elles offrent un registre permanent et sûr, il est possible d'utiliser la chaîne de blocs bitcoin à d'autres fins non financières. Diverses applications non monétaires peuvent ainsi être explorées et menées à bien, comme le vote ou la protection des brevets. Bien que ce type d'approche empêche le développeur d'incorporer des fonctions sur mesure comme il pourrait le faire dans sa propre version de la chaîne de blocs, elle a l'avantage d'offrir une infrastructure stable et accessible à moins coût, ce qui en fait un excellent terrain d'expérimentation de nouvelles idées. D'autres monnaies fondées sur les chaînes de blocs sont apparues dans le but explicite de permettre des applications plus variées. Prenons l'exemple du système Ethereum, qui a été créé d'après le livre blanc de Vitalik Buterin et grâce à une campagne de financement participatif. Il comporte une monnaie, l'ether, décrite comme en étant le carburant, ainsi qu'un code qui peut être utilisé afin de mettre en œuvre un large éventail de fonctions non financières, tels que les contrats intelligents, la gestion des droits numériques ou encore les organisations autonomes décentralisées.

Incidences et évolutions possibles

En 2014, un avis de l'Autorité bancaire européenne a mis en lumière certains des risques que présentent les devises fondées sur les chaînes de blocs. D'après cet avis, leurs atouts immédiats, notamment les transferts rapides, sûrs et peu coûteux, ne présentent que peu d'intérêt pour l'Union européenne, où les transferts conventionnels offrent déjà une grande partie de ces avantages. Pour beaucoup d'utilisateurs, les véritables atouts de ces monnaies, au-delà des économies modestes en temps et en argent, résident dans les fonctionnalités et les valeurs qui font défaut aux devises traditionnelles. Ces avantages peuvent inclure quelques-uns des «problèmes» très médiatisés du bitcoin, à savoir sa grande volatilité et son utilisation sur les marchés illégaux du Dark Web, qui pourraient bien tous deux avoir attiré de nombreux utilisateurs. En termes simples, s'il n'y avait aucun avantage sérieux à utiliser de telles cryptomonnaies en Europe, leur taux d'utilisation serait négligeable. Leur adoption continue cependant de croître, et ce malgré l'importante violation de sécurité qui a ébranlé les fondations idéologiques d'Ethereum.

Ces devises se trouvent déjà à la pointe du développement des chaînes de blocs, ce qui pourrait aboutir à un bouleversement techno-social majeur. En effet, si elles se montrent à la hauteur de leurs ambitions, les cryptomonnaies pourraient ouvrir la voie à un processus de décentralisation à travers lequel les institutions qui régissent traditionnellement le système financier, comme les États et les banques, perdraient de leur pouvoir. Cependant, ces mêmes détenteurs du pouvoir financier travaillent aujourd'hui à la recherche et au développement de chaînes de blocs qui répondent à leurs propres besoins. Ces chaînes pourraient s'avérer moins décentralisées et transparentes que les autres.

Toujours est-il que les principales conséquences des devises basées sur les chaînes de blocs apparaîtront peut-être dans des domaines extérieurs au système financier. Le bitcoin et *ses homologues* offrent un large socle d'utilisateurs, des espaces propices à l'expérimentation et un «carburant» pour faire progresser ces idées. Même si le bitcoin ne révolutionne pas le système financier, il pourrait ouvrir la voie à d'autres applications susceptibles de procurer, par exemple, de formidables avantages pour les chaînes d'approvisionnement et les services publics. Si le large éventail d'applications des chaînes de blocs fait aujourd'hui l'objet de nombreuses discussions, les devises telles que le bitcoin ont occupé, ces dernières

années, une place centrale dans les médias et les décisions politiques, ce qui pourrait avoir une influence sur l'évolution de la technologie. Autrement dit, les références fréquentes à la valeur fluctuante du bitcoin et à son utilisation sur les marchés noirs pourraient détourner les acteurs concernés et le public d'un débat plus productif au sujet des nombreuses possibilités et des multiples défis liés à cette technologie.

Élaboration d'une politique d'anticipation

Les monnaies virtuelles présentent un grand nombre de problèmes juridiques et réglementaires, y compris en ce qui concerne les mécanismes de protection des consommateurs, les méthodes d'application de la loi et la possibilité de commettre des activités illégales comme la fraude fiscale ou la vente de produits illégaux. Elles peuvent aussi apporter de nombreux avantages aux citoyens, comme une réduction des coûts, une sécurité accrue et un système financier innovant et plus accessible. Ces questions, parmi d'autres, ont été reconnues dans une résolution récente du Parlement européen, laquelle souligne également les possibilités offertes par la technologie de la chaîne de blocs «bien au-delà du seul secteur financier» et appelle à l'adoption d'une approche réglementaire proportionnée ainsi qu'à un renforcement des capacités et de l'expertise au niveau de l'Union.

2. Contenu numérique: chaînes de blocs et gestion des droits

La contrefaçon et la fraude dans le domaine de l'art sont des disciplines anciennes, mais, à l'époque de l'internet, il suffit souvent d'un simple copier-coller. Des contenus multimédias ont été copiés et partagés à grande échelle, souvent de manière illégale, depuis que les systèmes haute fidélité domestiques permettent de copier facilement des disques vinyles et des émissions de radio sur des cassettes audio. L'internet a rendu le piratage encore plus facile. Les pionniers s'étaient organisés en réseaux mondiaux en vue de partager des copies de CD par la poste. L'augmentation de bande passante et l'apparition des formats numériques ont permis aux réseaux de partage de fichiers de faire connaître le piratage au grand public. Aujourd'hui, le piratage de contenus multimédias se fait en général au moyen de «torrents» et, de plus en plus, par streaming. Malgré le caractère souvent illégal de cette distribution de contenu, la pratique est si répandue et sa répression si difficile que la mise en conformité est souvent considérée comme facultative. Récemment, les services d'abonnement légaux ont supplanté une partie de ce piratage en proposant un accès à des contenus multimédias en contrepartie d'une redevance versée aux ayants droit à partir des revenus perçus sur les abonnements et la publicité. Cependant, aucun modèle de distribution, jusqu'à l'arrivée de la chaîne de blocs peut-être, n'est parvenu à apporter une réponse efficace aux réalités des échanges illégaux de contenus numériques à l'ère de l'internet, en tenant compte des intérêts de l'auteur original, du consommateur et des divers intermédiaires.

Lorsque les consommateurs achètent des livres ou des disques, ils entrent en possession d'un objet physique qu'ils peuvent ensuite vendre, céder ou léguer dans le cadre d'un héritage. Leurs droits sont toutefois limités: par exemple, ils ne doivent pas en distribuer de copies et ils sont tenus de verser une redevance s'ils en diffusent le contenu. En achetant l'équivalent numérique de ce même contenu médiatique, les consommateurs savent qu'ils n'acquièrent pas la propriété d'un objet physique, mais beaucoup ne se rendent pas compte qu'ils n'acquièrent pas non plus la propriété du contenu. Au contraire, ils concluent un contrat de licence valide pour une période donnée ou un certain nombre de lectures. Ces licences ne peuvent être vendues, cédées ni même léguées en héritage. La constitution d'une collection numérique légale de musique, de livres, de jeux et de films coûte souvent autant que celle d'une collection de disques et de livres au contenu équivalent. Cela représente un investissement considérable tout au long de la vie, mais qui ne peut pas être cédé et qui disparaît au moment du décès. Alors que les générations précédentes pouvaient prendre plaisir à revivre les goûts et les souvenirs de leurs êtres chers au moyen de leurs vieux cartons de disques, de livres et de jeux, les enfants d'aujourd'hui pourraient ne pas jouir du même accès aux contenus numériques de leurs parents. La

technologie de la chaîne de blocs pourrait-elle résoudre ces problèmes et d'autres questions en matière de contenus numériques?

Comment la chaîne de blocs pourrait permettre de gérer les droits numériques

La technologie de la chaîne de blocs pourrait servir à la gestion des droits du consommateur associés aux produits numériques. Dans la plupart des cas, il est question d'œuvres reproduites en masse qui sont l'équivalent numérique des CD, DVD et des livres, et dont l'auteur vend de nombreuses copies. Cependant, la technologie pourrait également trouver son application dans le domaine émergent des œuvres numériques uniques, à savoir, par exemple, l'équivalent numérique d'un tableau. Dans ce cas de figure, l'acheteur n'acquiert pas une version dérivée, comme le MP3 d'une chanson, mais les droits exclusifs de l'œuvre originale elle-même. La chaîne de blocs peut protéger à la fois les consommateurs et les auteurs de toutes sortes d'œuvres numériques en consignant l'historique de propriété des contenus numériques, voire en garantissant le respect des droits numériques.

Elle peut également servir à consigner l'ensemble des ventes, des prêts, des dons et autres transferts d'objets numériques individuels. Toutes les transactions sont observées et validées par l'ensemble des utilisateurs. Suivant le même principe que pour les transactions sur un compte en banque ou un registre cadastral, les objets ne peuvent pas être transférés tant qu'ils ne sont pas légitimement détenus. Les acheteurs peuvent vérifier qu'ils acquièrent bien des copies légitimes de fichiers MP3 et vidéo. Le registre des transactions permet en effet de confirmer que les différents transferts de propriété remontent bien jusqu'au propriétaire d'origine, c'est-à-dire l'auteur de l'œuvre. Ce concept pourrait être couplé à celui des contrats intelligents pour que les utilisateurs puissent octroyer à d'autres l'accès au contenu pendant une durée limitée avant que les droits ne soient automatiquement rendus au propriétaire, ou pour que les dispositions testamentaires soient automatiquement exécutées à l'enregistrement d'un certificat de décès. Pour qu'un tel système fonctionne, il est fondamental que le transfert de propriété d'une partie à une autre entraîne la perte d'accès pour l'ancien propriétaire, comme cela arrive lors de la vente d'un disque vinyle d'occasion. En effet, il convient de connaître autant le moment auquel prennent fin les droits d'un utilisateur que celui auquel s'ouvrent les droits d'un autre. Or, la chaîne de blocs permet justement de vérifier l'identité du propriétaire du contenu ainsi que l'historique de propriété. De cette manière, les consommateurs pourraient s'assurer qu'ils achètent des biens numériques légitimes plutôt que des copies illégitimes, et les ayants droit pourraient faire valoir leurs droits. La vérification de la légitimité de la propriété pourrait être effectuée au moyen de la technologie, par des appareils qui vérifieraient les droits selon le profil de l'utilisateur avant de démarrer la lecture. Cela nécessiterait de développer de nouveaux codecs, d'élaborer de nouvelles normes pour le secteur et de mettre au point des formats de fichiers qui regroupent contenu et permissions.

Outre l'achat de copies sous licence d'œuvres numériques, comme des chansons MP3, il est également possible d'acheter et de vendre des œuvres originales, c'est-à-dire l'œuvre elle-même. Tout comme l'achat d'un tableau donne davantage de droits que l'achat de la reproduction d'un tableau, l'acheteur d'une œuvre numérique originale acquiert également les droits exclusifs de diffuser le contenu, d'en vendre des copies et d'intenter des actions à l'encontre des personnes qui en font un usage illégal. Il est important pour l'acheteur de savoir s'il acquiert la propriété de l'œuvre assortie de sa valeur et de ses droits, ou juste une reproduction sous licence pour son usage personnel. Dans ce cas, la chaîne de blocs pourrait servir à vérifier l'identité du véritable propriétaire du contenu, la nature de ce contenu (exemplaire original ou copie) et l'ensemble des droits qui l'accompagnent.

En sus des droits des vendeurs et des acheteurs, la chaîne de blocs pourrait garantir la protection des droits de l'auteur de l'œuvre, qui pourrait choisir de conserver une partie de ces droits lors de la vente de son contenu. Ces créateurs originaux pourraient constituer un réseau complexe d'acteurs détenant une propriété partielle et un droit au versement d'une redevance lorsque le contenu est utilisé à des fins commerciales. Dans le cas de morceaux de musique, par exemple, ce groupe pourrait comprendre les compositeurs, les musiciens et les autres artistes, ainsi que les ingénieurs d'enregistrement, les managers

et toute une équipe d'intermédiaires spécialisés. Les droits de chacun de ces acteurs, de même que les modalités et les mécanismes de versement, peuvent être encodés numériquement en vue de garantir un paiement plus fiable et efficace. Le paiement des droits d'auteur pourrait même être effectué de manière automatique au moyen de contrats intelligents.

Incidences et évolutions possibles

Une telle utilisation de la technologie de la chaîne de blocs pourrait, pour la première fois, permettre aux consommateurs d'acheter et de vendre des copies numériques d'occasion, de les offrir ou de les donner à des magasins caritatifs, de les prêter à des amis ou de les inscrire à leur héritage, comme c'était le cas avec les disques vinyle et les livres, sans que se propage pour autant une multitude de copies non autorisées. Pour qu'une telle méthode de gestion des droits numériques fonctionne là où tant d'autres ont échoué, la chaîne de blocs doit parvenir à concilier les droits des vendeurs, des acheteurs, du réseau d'acteurs (qui inclut le propriétaire original du contenu) et d'un grand nombre d'autres intermédiaires, y compris les personnes qui développent et entretiennent la chaîne elle-même. Au vu de la complexité des réseaux d'intérêts en jeu, il serait idéaliste de s'attendre à voir apparaître rapidement une solution qui ne suscite aucune controverse, même si certains avancent que la technologie de la chaîne de blocs pourrait avoir une véritable incidence sur le secteur musical d'ici 10 à 15 ans tout en offrant davantage de possibilités aux premiers à l'adopter.

Élaboration d'une politique d'anticipation

Le droit continuera de jouer un rôle important dans l'identification des œuvres protégées par le droit d'auteur et dans la résolution des litiges. Le développement des chaînes de blocs dans ce domaine pourrait aboutir à des politiques de licence multiterritoriales et au renforcement de la sécurité juridique des créateurs et des acheteurs, tout en offrant des mécanismes efficaces de résolution des litiges, notamment en ce qui concerne les tarifs, les conditions de concession des licences, les mandats relatifs à la gestion des droits en ligne et le retrait des droits.

3. Brevets: protéger les inventeurs tout en encourageant l'innovation

Les brevets donnent à leur titulaire le droit exclusif d'exploiter des innovations pendant une durée donnée. Le système des brevets a été conçu pour encourager l'innovation en offrant aux inventeurs une longueur d'avance sur leurs concurrents afin de pouvoir tirer profit de leurs idées. Après tout, pourquoi investir le temps et l'argent nécessaires à la mise au point d'une idée si d'autres peuvent la copier et dégager des bénéfices immédiatement sans avoir contribué aux coûts de développement? Cependant, protéger les innovateurs ne signifie pas la même chose qu'encourager l'innovation. Le système des brevets doit trouver le juste milieu entre protection des innovateurs et protection des concurrents. Si les inventeurs ne sont pas protégés, l'exposition à une concurrence débridée freine l'investissement dans l'innovation. En revanche, si les concurrents ne sont pas protégés, ils sont découragés d'investir dans des améliorations et des économies de coûts, voire empêchés d'entrer sur le marché et de briser le monopole de l'inventeur d'origine. Fondamentalement, le système des brevets peut être vu comme un échange par lequel l'État cède aux inventeurs un monopole, d'une portée et d'une durée limitées, pour qu'ils puissent exploiter leur invention en contrepartie de la publication par ceux-ci du fonctionnement détaillé de l'invention, ce qui permet à d'autres de concevoir des améliorations ou des solutions différentes.

Toutefois, le système des brevets présente plusieurs problèmes bien connus. Par exemple, les concurrents peuvent parfois tirer parti du brevet avant l'inventeur, soit parce que le brevet n'est pas assez solide ou parce que ses titulaires n'ont pas les moyens de se défendre contre sa violation. Cette situation, associée aux dépenses liées à l'obtention de brevets dans différentes régions, pousse certaines

entreprises à prendre le risque de commercialiser leurs inventions sans aucune protection par brevet. Un autre problème réside dans la complexité du système de brevets. Chaque pays possède ses propres principes et systèmes en matière de brevets. Malgré les récentes avancées, il n'existe toujours pas de brevet unitaire européen. Néanmoins, l'Office européen des brevets propose un guichet unique qui permet de déposer des brevets dans l'ensemble des systèmes des États membres, mais les frais de traduction, de validation et de renouvellement dans les différents systèmes rendent le processus relativement onéreux en Europe.

Le système des brevets pose également le problème des chasseurs de brevets, qui n'inventent rien mais acquièrent des brevets et demandent ensuite réparation en cas de violation. Bien que leurs réclamations n'aient pas toujours une assise juridique solide, les entreprises sont souvent incapables ou peu désireuses d'engager les dépenses juridiques nécessaires à leur défense et préfèrent s'arranger à l'amiable. Les autorités européennes en matière de concurrence enquêtent de plus en plus sur de tels abus, notamment dans le secteur de la haute technologie.

Alors que le système des brevets est en grande partie numérisé aujourd'hui, il n'a pas connu de changement structurel majeur depuis l'avènement de la révolution numérique. Selon certains, le recours à une chaîne de blocs en lieu et place des brevets pourrait, d'une part, fluidifier l'innovation en réduisant le nombre de différends contractuels et, d'autre part, permettre de pallier quelques-unes des faiblesses du système de brevets. La section qui suit vise à expliquer le rôle que la chaîne de blocs pourrait avoir dans le système des brevets et énumère les bénéfices potentiels, avant de présenter un tour d'horizon des idées plus radicales selon lesquelles la chaîne pourrait se substituer au système des brevets, voire précipiter sa disparition.

Comment la chaîne de blocs pourrait contribuer au système des brevets

Deux caractéristiques de la technologie de la chaîne de blocs la rendent particulièrement adaptée au système des brevets: le «hachage» et la «preuve d'existence». La première, le hachage, est un procédé qui consiste à calculer à partir d'un document un code de longueur fixe, décrit comme une empreinte numérique, appelée plus souvent «hash» ou condensé. Tous les condensés sont uniques: la plus petite différence, tel un accent manquant sur une lettre dans un long document, se traduit par l'obtention d'un condensé intégralement différent. Ce n'est qu'en répétant le hachage sur une copie identique au document original que l'on obtient le même condensé. Surtout, il est impossible de recréer un document à partir de son condensé. La deuxième, la preuve d'existence, consiste à enregistrer ces condensés dans la chaîne de blocs. Dès lors, une entrée est créée qui prouve que le condensé existait à un moment donné. N'importe qui peut vérifier cette entrée, mais personne ne peut interpréter le contenu du condensé. Cependant, les détenteurs du document original peuvent prouver que ce document existait au moment de la transaction en répétant le procédé de hachage sur une copie identique dudit document. Si le même algorithme de hachage produit le même condensé, cela indique qu'ils sont en possession du même document. Cette méthode offre la possibilité intéressante d'enregistrer de manière publique l'existence d'un document sans en révéler le contenu. Pour certains, les inventeurs pourraient utiliser ce procédé afin de protéger leur travail en enregistrant un condensé de la description de leur brevet, d'un texte ou d'un extrait de code informatique dans la chaîne de blocs. Aussi, des services de preuve d'existence sont déjà disponibles dans le domaine de la protection des brevets. Ces services sont adossés aux capacités des chaînes existantes, notamment la chaîne du bitcoin, mais un système sur mesure d'enregistrement des condensés pourrait être mis au point et déployé spécialement en vue d'établir la preuve d'existence.

Incidences et évolutions possibles

Le recours à la technologie de la chaîne de blocs dans le cadre du système des brevets pourrait pallier efficacement les faiblesses en matière d'enregistrement et d'harmonisation de l'horodatage de cet enregistrement, et ce pour plusieurs systèmes nationaux de brevets. Des services de preuve d'existence fondés sur la chaîne de blocs pourraient être proposés en tant que première étape du processus de dépôt

de brevet. Le processus pourrait ensuite être rationalisé et sécurisé, ce qui rendrait ses étapes plus transparentes pour le déposant tout en réduisant les possibilités de corruption. Cependant, si l'amélioration du processus d'enregistrement et d'horodatage des inventions pourrait apporter des avantages concrets au système des brevets, les problèmes les plus sérieux, tels que ceux des chasseurs de brevets et des coûts de traduction, nécessiteront peut-être une solution différente.

Certains ont avancé (à tort) qu'un brevet n'est rien de plus qu'un «concept tamponné et conservé dans un endroit où il ne peut être falsifié». Il a même été suggéré que la chaîne de blocs pourrait remplacer le système des brevets tout en permettant aux inventeurs de conserver leurs secrets. En fait, la publication des brevets est l'un des éléments essentiels de leur fonction: stimuler l'innovation. La publication des brevets encourage les concurrents à concevoir d'autres solutions ainsi que des améliorations en vue de briser le monopole après expiration du brevet, tout en suscitant des avancées dans des domaines qui ne sont pas couverts par le brevet. L'enregistrement de l'inventeur et de la date d'une idée n'est qu'une partie infime du travail qu'effectuent les intermédiaires des offices de brevets. Les agents des offices de brevets évaluent la nouveauté des brevets déposés, vérifient leur conformité aux règlements et aux politiques de la région et publient des archives consultables des brevets acceptés, le tout constituant un important travail que la technologie de la chaîne de blocs ne saurait remplacer.

Élaboration d'une politique d'anticipation

Les systèmes de brevets actuels pourraient devenir plus efficaces à l'aide de la technologie de la chaîne de blocs, qui pourrait également permettre aux offices de brevets d'offrir des services de preuve d'existence à moindre coût. Cependant, il convient de souligner que la preuve d'existence au moyen de d'une chaîne de blocs, ou même par tout autre moyen, ne saurait être considérée comme équivalant à la protection par brevet. Pour que les services de preuve d'existence fournis par des tiers, par exemple ceux qui reposent sur la chaîne de blocs du bitcoin, soient considérés comme des registres légitimes, ils devront être reconnus par les organes pertinents.

4. Vote électronique: vers une révolution du système électoral?

En dépit de la numérisation de nombreux aspects importants de la vie moderne, les élections se tiennent encore largement hors ligne, sur du papier. Depuis le début du siècle, le vote électronique est considéré comme une avancée prometteuse, voire inévitable, qui pourrait accélérer et simplifier les élections et en réduire le coût. Il est en effet vu comme un moyen potentiel d'augmenter la mobilisation et le taux de participation, et même de rétablir les liens entre les citoyens et les institutions politiques – des arguments parfois accueillis avec un certain scepticisme. Le vote électronique peut se dérouler de différentes façons: par internet ou un réseau isolé dédié; en demandant aux votants de se rendre dans un bureau de vote ou en permettant le vote sans supervision; au moyen d'appareils existants, comme les téléphones et ordinateurs portables, ou avec du matériel spécialisé. Aujourd'hui, une autre question se pose: faut-il continuer de faire confiance aux autorités centrales, ou faut-il avoir recours à la technologie de la chaîne de blocs pour mettre à la disposition des citoyens un registre de vote ouvert? De nombreux experts s'accordent à dire que l'organisation d'un vote électronique à l'occasion d'élections nationales nécessiterait des avancées révolutionnaires en matière de systèmes de sécurité. Cependant, de nombreux autres types de scrutins régionaux et au sein des organisations pourraient être numérisés plus facilement au moyen de la chaîne de blocs, ce qui faciliterait la participation d'un plus grand nombre de personnes à la prise de décisions importantes, à l'adoption de stratégies à long terme, aux choix d'investissement et aux nominations à différents postes.

Comment la technologie de la chaîne de blocs pourrait être utilisée dans le cadre du vote électronique

La chaîne de blocs est un moyen de tenir et de vérifier un registre qui est transparent et distribué entre les utilisateurs. Habituellement, les votes sont enregistrés, gérés, comptabilisés et vérifiés par une autorité centrale. Le vote électronique à chaîne de blocs (Blockchain-enabled e-voting ou BEV) donnerait aux électeurs eux-mêmes les moyens d'effectuer ces tâches en leur permettant d'obtenir leur propre copie du registre des votes. Ce registre ne pourrait pas être modifié, étant donné que les autres votants seraient capables de déceler toute différence avec leur version. Un bulletin frauduleux ne pourrait pas non plus être ajouté, car les autres électeurs pourraient s'apercevoir qu'il n'est pas compatible avec les règles du vote, que ce soit parce qu'il a déjà été comptabilisé ou parce qu'il n'est pas associé à un électeur valide. Le système BEV réduirait ainsi le pouvoir et la responsabilité des acteurs centraux comme les autorités électorales, au profit d'un consensus communautaire fondé sur la technologie.

Il est possible de mettre au point des systèmes BEV en élaborant un nouveau mécanisme spécialement conçu pour prendre en compte les caractéristiques propres à l'élection et aux électeurs. Une autre approche qui pourrait être plus simple et moins coûteuse serait d'utiliser une chaîne déjà établie, telle que le bitcoin. Étant donné que la sécurité d'un registre distribué repose sur l'ampleur de sa base d'utilisateurs, une telle approche pourrait également s'avérer plus sûre dans le cadre d'élections mineures au sein d'organisations qui comptent un nombre restreint de votants et possèdent des moyens limités pour développer un système idoine.

Le système BEV présente le plus grand potentiel pour les élections tenues dans des organisations. Il a déjà été utilisé dans le cadre d'élections internes de partis politiques au Danemark et pour le vote d'actionnaires en Estonie. Pour aller plus loin, le BEV pourrait être associé à des contrats intelligents, afin de déclencher des actions automatiquement si certaines conditions sont réunies. Par exemple, les résultats d'une élection pourraient entraîner la mise en œuvre automatique de promesses électorales, de choix d'investissement ou d'autres décisions organisationnelles.

De nombreux analystes considèrent que la chaîne de blocs pourrait favoriser des transformations plus profondes, par exemple dans le cadre des débats relatifs aux administrations virtuelles, aux systèmes techno-démocratiques ou à la possibilité plus distante de recourir au système BEV lors d'élections nationales. Des idées ambitieuses évoquent la possibilité d'utiliser la chaîne de blocs pour mettre en place une démocratie «liquide», qui associerait la démocratie directe (au titre de laquelle les citoyens votent régulièrement pour des décisions stratégiques spécifiques) et un système de délégués (qui permettrait aux citoyens de voter eux-mêmes sur ces questions ou de déléguer leur vote à n'importe quel autre citoyen, que ce soit un politique, un journaliste, un scientifique ou un ami de confiance, et de retirer ou réassigner ce mandat à tout moment).

Incidences et évolutions possibles

Dans le cadre d'élections mineures et de décisions au sein d'organisations, le BEV pourrait contribuer à établir une structure sociale plus participative et ascendante en offrant un système de vote électronique sûr et relativement peu coûteux. En ce qui concerne les suggestions plus ambitieuses vis-à-vis des élections nationales, les enjeux sont bien plus importants et la situation plus délicate. Certains ont remis en question le degré d'anonymat et d'accessibilité permis par le BEV et soulevé le problème de la coercition. Toutefois, bien que le BEV présente divers avantages par rapport au papier et aux autres systèmes de vote électronique, nombre des préoccupations qu'il soulève s'appliquent aussi bien aux systèmes traditionnels basés sur le papier. La *coercition* est un danger pour n'importe quel système de vote à distance, comme les votes postaux par exemple. La seule garantie à cet égard est l'isoloir, que ce soit pour le BEV ou le vote à bulletin papier. L'*accessibilité* de tous les électeurs est une autre préoccupation majeure de toute élection. Selon le type d'interface, le BEV pourrait être considéré par certains électeurs comme trop compliqué, a fortiori si le système est entièrement décentralisé et permet

d'accéder aux données afin de vérifier que les procédures ont été correctement suivies. L'*anonymat* est souvent considéré comme étant un élément clé de la participation démocratique, bien que certaines élections nationales ne soient pas entièrement anonymes. Le Royaume-Uni, par exemple, dispose d'un système de vote papier sous pseudonyme, où chaque bulletin est lié par un code à une entrée sur la liste électorale. Dans ce cas, les électeurs n'ont pas d'autre choix que de faire confiance aux autorités électorales pour la protection de leur anonymat. Même s'il est difficile de découvrir sur qui les votes se sont portés, cela reste possible. Comme le BEV est également un vote sous pseudonyme, il serait éventuellement possible de pour qui une personne a voté. Des travaux sont menés afin d'apporter une réponse technique à ce problème en développant des systèmes de BEV qui garantissent un anonymat total. Une autre méthode pourrait consister à confier à une autorité centrale la responsabilité d'affecter les pseudonymes utilisés dans le cadre d'un scrutin par BEV et de les garder secrets, comme c'est le cas aujourd'hui pour le système de vote papier du Royaume-Uni. Le système ferait ainsi l'objet d'un certain degré de centralisation, qui pourrait toutefois être acceptable dans le cadre d'élections nationales.

Une autre question qui se pose est celle de la marche à suivre en vue d'instaurer une confiance généralisée envers la sécurité et la légitimité du système. Tout comme c'est le cas pour les élections papier, il ne suffit pas que le résultat soit juste et valide. L'électorat dans son ensemble, même s'il est déçu du résultat, doit accepter que le processus est légitime et fiable. Ainsi, au-delà de la sécurité et de la précision qu'il doit apporter, le BEV doit également inspirer confiance. La complexité du protocole de la chaîne de blocs pourrait être un frein à l'acceptation du BEV par le grand public.

L'analyse des effets potentiels du BEV doit prendre en compte les valeurs et les politiques que ce système promeut. Le BEV est plus qu'une simple numérisation du processus électoral traditionnel: il propose une méthode de vote qui s'accompagne d'un ensemble différent de valeurs et de fondements politiques. Traditionnellement, les pouvoirs publics organisent les élections et le processus est opaque, centralisé et descendant. Le BEV propose l'inverse. Le processus est géré par le peuple et il est transparent, décentralisé et ascendant. Alors que la participation aux élections classiques renforce l'autorité de l'État, la participation au BEV assoit la primauté du peuple. Ainsi, il n'est guère surprenant que des liens soient établis entre le BEV et la transition vers une démocratie plus directe, décentralisée et ascendante, ainsi que vers la démocratie «liquide» susmentionnée. Dans tous les cas, l'importance que prendra la technologie de la chaîne de blocs dans le domaine du vote électronique dépendra de sa capacité à refléter les valeurs et les structures de la société, de la politique et de la démocratie.

Élaboration d'une politique d'anticipation

Même si les organisations sont largement libres de tenir des élections au moyen de la chaîne de blocs si tel est leur désir, elles doivent cependant se conformer aux lois européennes en matière de confidentialité et de sécurité des données. Bien que le droit européen ne dispose pas de protocoles définis pour la tenue des élections politiques dans les États membres, une convergence s'est opérée et des efforts ont été consentis afin d'encourager l'utilisation du vote électronique dans le respect des principes constitutionnels de la loi électorale (suffrage universel direct, libre, secret et équitable).

5. Contrat intelligents: là où le code informatique fait loi

Les registres distribués présentent plusieurs caractéristiques intéressantes et innovantes par rapport aux registres centralisés. Toutefois, au-delà de la simple consignation de l'horodatage et des détails des transactions, ils peuvent également jouer un rôle plus actif, voire autonome, dans la gestion et l'exécution des transactions. En incorporant du code informatique à la chaîne de blocs, des transactions peuvent être exécutées automatiquement lorsque certaines conditions sont remplies, ce qui offre une «garantie d'exécution». Ces contrats intelligents qui s'exécutent automatiquement en tirant parti de cette fonctionnalité connaissent un développement rapide. Toutefois, des questions se posent concernant la frontière entre le code informatique et la loi.

Comment fonctionnent-ils?

Bien que les contrats intelligents puissent faire référence à plusieurs concepts différents, ils ont été définis en 1994 comme des protocoles de transactions informatiques qui exécutent les modalités d'un contrat – une définition qui reste d'actualité dans le contexte de la technologie de la chaîne de blocs. Sous leur forme la plus simple, les modalités d'un accord entre deux ou plusieurs parties sont programmées dans du code informatique (jeu d'instructions) qui est inscrit dans une chaîne de blocs de la même manière que les transactions sont normalement enregistrées dans d'autres chaînes. Lorsque certaines conditions décrites dans le code sont remplies, des actions spécifiques, elles aussi définies dans le code, sont automatiquement déclenchées. Ainsi, par exemple, la livraison de produits pourrait déclencher une instruction de paiement. Cela pourrait ensuite déclencher d'autres actions contenues dans d'autres contrats intelligents, par exemple en vue d'échanger des devises ou de passer d'autres commandes le long de la chaîne d'approvisionnement. Bon nombre des cas proposés d'applications à court terme se rencontrent dans le secteur financier, par exemple dans le cadre de prêts et de produits d'assurance qui mobilisent d'importantes ressources manuelles qui pourraient être automatisées. Les contrats intelligents pourraient être la clé de l'automatisation des successions, pour lesquelles l'enregistrement du certificat de décès déclencherait la distribution des biens, y compris des contenus numériques.

La chaîne de blocs Ethereum propose son propre langage de programmation et sa propre monnaie, qui ont été spécialement conçus pour les contrats intelligents. D'autres systèmes de contrats intelligents reposent sur d'autres chaînes de blocs, y compris celle du bitcoin. À l'heure actuelle, la mise en place de contrats intelligents demande un certain effort et entraîne des dépenses, ce qui les rend plus adaptés à des accords répétitifs plutôt qu'à des contrats ponctuels. Au vu de leur nature prédéterminée, ils sont inappropriés aux situations qui sont sujettes à des changements importants pendant la durée du contrat. Ainsi, au vu du degré d'incertitude juridique, il serait plus prudent de restreindre les contrats intelligents à des relations relativement consensuelles et à des accords qui courent peu de risques d'être contestés par l'une ou l'autre des parties. Enfin, étant donné qu'ils réagissent à des stimuli numériques et déclenchent d'autres procédures numériques, ils sont particulièrement efficaces dans les situations où les différentes modalités et conséquences des clauses sont elles aussi de nature numérique, et sont donc particulièrement adaptés à l'automatisation numérique.

Incidences et évolutions possibles

Étant donné le caractère immuable de la chaîne de blocs, le code sur lequel les parties s'accordent, et donc le contrat qui les lie, peut seulement être annulé ou modifié selon des termes contenus dans le code lui-même. Les contrats traditionnels offrent le choix de payer ce qui est dû conformément aux stipulations du contrat, ou de ne pas remplir ses obligations contractuelles et de faire face aux conséquences, par exemple sous la forme d'une action en justice. Cependant, ce choix n'existe plus dans un contrat intelligent au paiement automatisé, car la transaction est exécutée systématiquement.

Une interprétation radicale des contrats intelligents réduirait le contrat à son code informatique, ce qui équivaut à déclarer que le code fait loi: il est autonome, automatiquement exécuté et automatiquement appliqué. Ce pourrait être la position d'une frange «extrémiste» du mouvement populaire qui soutient la chaîne de blocs, qui se placerait alors au-delà du contrôle exercé par les structures en place telles que les États et les juridictions. Lorsque le code informatique est considéré comme étant la loi, toute erreur ou vulnérabilité accidentelle devient elle-même partie du contrat. L'exploitation de ces bogues en vue de prendre le contrôle de biens ne pourrait être jugée comme un vol, car l'erreur qui l'aurait permise ferait partie du code et donc, par définition, de la «loi». Les contrats intelligents pourraient également contenir des clauses illégales, comme dans le cas d'un code de distribution de succession qui ne s'acquitterait pas des droits de succession prévus par la juridiction concernée.

Une interprétation plus réaliste des contrats intelligents consiste à les intégrer au système juridique existant. Tout comme pour les contrats papier, des clauses supplémentaires peuvent être imposées, et

d'autres peuvent être annulées ou réinterprétées selon l'intention des parties et d'après les principes généraux de la loi. La loi du pays l'emporte toujours sur la «loi» inscrite dans le code informatique, y compris dans les cas où les procédures judiciaires et l'application des décisions pourraient s'avérer difficiles. Ainsi, bien qu'il soit largement reconnu que les contrats intelligents apporteront des gains d'efficacité dans différents domaines, il est peu probable qu'ils remplacent le droit contractuel traditionnel ou les avocats spécialisés dans les contrats.

À la différence des chaînes de blocs simples qui enregistrent des transactions, les chaînes qui incorporent du code exécutable présentent un degré supplémentaire de complexité et nécessitent davantage d'intervention. Elles pourraient ainsi demander plus de puissance de calcul pour le minage et l'entretien du système, ce qui pourrait entraîner des coûts d'utilisation plus élevés, y compris en énergie. Cette complexité pourrait également exposer les chaînes de blocs à un plus grand nombre de risques de sécurité, ce qui, en conjonction avec l'idéologie selon laquelle «le code fait loi», pourrait confronter les contrats intelligents à de graves problèmes pratiques. Ces problèmes pourraient se dissiper au fur et à mesure de l'élaboration des normes et de l'apparition de la première génération «d'avocats intelligents», formés et rompus à la gestion des contrats intelligents.

Élaboration d'une politique d'anticipation

Plusieurs pans de la loi risquent d'être exploités dans les cas où le contrat n'est pas considéré comme relevant d'une juridiction traditionnelle. Citons par exemple la fiscalité (des salaires, des ventes, des successions et des plus-values), l'exploitation (en matière de location et de contrat de travail) et la criminalité d'entreprise (en ce qui concerne la fixation des prix et le délit d'initié). Il pourrait être nécessaire de trouver de nouveaux moyens d'affirmer la primauté du droit national dans le cas où l'automatisation des contrats intelligents rend l'application de la loi difficile. L'application des procédures judiciaires traditionnelles aux contrats intelligents pourrait faire naître de nouvelles responsabilités étatiques, comme l'arbitrage dans les situations où des bogues sont décelés dans le code du contrat. En transcrivant les accords au sein du code exécutable, les programmeurs prendraient des décisions quant aux modalités pratiques de leur mise en œuvre, ce qui leur conférerait une plus grande responsabilité aux yeux de la loi.

Les contrats intelligents peuvent s'avérer peu souples et peu à même de s'adapter à l'évolution des circonstances ou des désirs des parties. Toutes les questions ne peuvent pas trouver une réponse à l'avance, et il se produira toujours des imprévus qui nécessiteront d'interpréter la façon d'appliquer les clauses contractuelles. Le code informatique est tout simplement trop rigide pour permettre l'exécution algorithmique de tous les contrats. Le règlement des litiges contractuels et l'application des clauses contractuelles pourraient se compliquer au fur et à mesure des évolutions dans le domaine.

Le droit traditionnel des contrats, notamment la règle de conservation des documents et la règle de la preuve, pourraient nécessiter des modifications en vue de prendre en compte la nature automatisée et déterministe des contrats intelligents, de même que les problèmes soulevés par leur validité et leur force exécutoire. Le droit doit répondre aux difficiles questions qui se posent vis-à-vis du lien à établir avec le monde physique, réaliser les procédures de validation nécessaires et garantir la conformité des applications de la chaîne de blocs à la législation en vigueur. Le code informatique doit-il être vu comme la forme de droit la plus tangible, comme le considère Lawrence Lessig? Il est clair que des critères doivent être définis afin de garantir la validité légale et la force exécutoire des contrats intelligents en vertu de la loi.

6. Chaînes d'approvisionnement: vers la transparence et la responsabilité?

Le commerce international s'appuie sur une chaîne d'approvisionnement estimée à 16 billions d'euros. Les biens sont produits et distribués au moyen d'un vaste réseau de producteurs, détaillants, distributeurs, transporteurs et fournisseurs organisé selon un agencement complexe de procédures régissant la gestion des contrats, des paiements, de l'étiquetage, de l'emballage, de la logistique et de la lutte contre la contrefaçon et contre la fraude.

L'ampleur et la complexité des systèmes en question entraînent des frais de transaction élevés, des erreurs et des décalages fréquents dans les formalités administratives effectuées à la main, ainsi que des pertes dues aux dégradations et aux vols tout au long du processus. Au rang des autres problèmes rencontrés, on compte les conditions de travail abusives ou dangereuses; les dégâts environnementaux causés par la mauvaise utilisation des ressources ainsi que par les processus d'extraction et de production illégaux; les faux et les imitations ainsi que les risques sanitaires entraînés par la mauvaise gestion de la chaîne d'approvisionnement. Ces problèmes trouvent souvent une illustration dans des incidents très médiatisés, par exemple au sein des chaînes d'approvisionnement de l'alimentation, du textile et des diamants. Certains estiment que les normes et les certifications ont eu un effet positif sur la différenciation du choix et la sensibilisation du consommateur, mais ces procédures demeurent en pratique très coûteuses et peu fiables, notamment dans les régions qui souffrent d'une corruption galopante. Les «chaînes de contrôle», qui garantissent l'origine de chaque produit ou matériau, restent fragmentées entre les organisations et vulnérables à la fraude et aux erreurs, même lorsque cette chaîne relie une entreprise certifiée à une autre. De plus en plus de voix s'élèvent pour demander des chaînes d'approvisionnement en biens et en services plus sûres, plus fiables et plus transparentes. Il s'agit de savoir si la technologie de la chaîne de blocs peut réellement améliorer le secteur actuel de l'approvisionnement et de la logistique en réduisant l'inefficacité opérationnelle et la fraude, voire en répondant à des défis majeurs comme les pratiques de travail contraires à l'éthique et la dégradation de l'environnement.

Comment la chaîne de blocs pourrait permettre de gérer les chaînes d'approvisionnement

Les applications de la chaîne de blocs pourraient permettre d'améliorer les chaînes d'approvisionnement en fournissant l'infrastructure nécessaire à l'enregistrement, à la certification et au suivi à moindre coût des biens transférés entre des parties souvent éloignées, qui sont reliées par une chaîne d'approvisionnement mais ne se font pas confiance pour autant. Chaque bien est identifié par un «jeton» qui peut être transféré sur la chaîne de blocs, chaque transaction étant vérifiée et horodatée au moyen d'une méthode chiffrée mais transparente. Les parties prenantes peuvent y accéder, qu'elles soient fournisseurs, vendeurs, transporteurs ou acheteurs. Les termes de chaque transaction restent irrévocables et immuables et peuvent être inspectés par tout un chacun ou par les auditeurs habilités. Les contrats intelligents pourraient également être employés pour automatiser le paiement ainsi que d'autres procédures.

Incidences et évolutions possibles

Plusieurs entreprises, innovateurs et administrateurs mènent déjà actuellement des expériences de tenue de registres distribués au sein de leurs chaînes d'approvisionnement. Everledger permet aux entreprises et aux acheteurs de suivre l'acheminement des diamants de la mine jusqu'à la bijouterie et de lutter contre la fraude aux assurances et la fraude documentaire. Pour chaque diamant, Everledger mesure 40 caractéristiques, comme la taille, la clarté, l'angle de la culasse et le lieu d'origine. Un numéro de série est généré pour chaque diamant, gravé à l'échelle microscopique, puis ajouté sous sa forme numérique

à la chaîne de blocs d'Everledger, qui recense aujourd'hui 280 000 diamants. Cela permet d'établir et d'entretenir un historique exhaustif de la propriété, qui facilite la lutte contre la fraude et apporte une aide aux policiers et aux enquêteurs d'assurance dans la recherche des gemmes volées. Les consommateurs peuvent alors prendre la décision d'acheter en toute connaissance de cause, et, par exemple, de limiter leur recherches aux diamants à l'historique «propre», sans fraude, vol, travail forcé ni intervention de vendeurs douteux liés à la violence, à la drogue ou au trafic d'armes.

L'entreprise sociale londonienne Provenance a créé une plateforme en temps réel qui récupère et détermine l'origine d'un bien en lui affectant un jeton, ou «passeport numérique», qui peut être suivi tout au long de la chaîne d'approvisionnement jusqu'à l'arrivée à destination. Cela pourrait servir à contrecarrer la fraude dans le cadre de la vente de biens à l'appellation d'origine protégée, comme c'est souvent le cas pour des spécialités régionales comme le vin et le fromage. SmartLog incorpore des contrats intelligents dans les conteneurs de marchandises pour suivre leur emplacement et leurs environs à des fins de planification des ressources. La chaîne de blocs est également utilisée en vue de minimiser les risques de paiement: certaines entreprises comme Skuchain et Fluent offrent ainsi des moyens reposant sur cette technologie pour le financement de la chaîne d'approvisionnement et les paiements. Par ailleurs, dans le cadre d'un autre projet, un système est en cours d'élaboration afin de rationaliser le traitement manuel des documents en établissant une chaîne de blocs privée pour partager les informations entre les exportateurs, les importateurs et leurs banques. Premier détaillant au monde, Wal-Mart met actuellement à l'essai la chaîne de blocs afin d'assurer la sécurité des aliments. S'il est précis et tenu à jour, un registre fondé sur la chaîne de blocs peut permettre l'identification d'un produit, d'une livraison et d'un vendeur, par exemple en cas d'intoxication, afin de déterminer où et quand la nourriture a été produite et qui l'a inspectée. Un registre précis pourrait également accroître l'efficacité de la chaîne d'approvisionnement, accélérant ainsi la livraison de la nourriture dans les magasins et réduisant le gaspillage et les déchets.

Les systèmes de chaîne de blocs possèdent les capacités nécessaires pour améliorer l'efficacité des procédures d'approvisionnement, de logistique et de paiement, réduire le traitement manuel des documents d'import/export, garantir la conformité et la livraisons des biens et éviter les pertes. Ils constituent, à ce titre, un moyen de réduire les coûts, d'améliorer la sécurité et de minimiser la fraude. Ils peuvent aussi permettre de vérifier l'authenticité et l'origine des biens et des services ainsi que leur conformité à des normes éthiques. Un historique de propriété transparent et traçable révélerait tout cas de fraude, de vol, de recours au travail forcé, tout lien avec la violence, la drogue, le trafic d'armes ou tout autre activité douteuse, ce qui renforcerait la capacité de faire respecter la loi et favoriserait une consommation plus responsable. Cependant, plusieurs raisons incitent à une certaine prudence. La confiance entre les participants repose sur la confiance vis-à-vis de la technologie de la chaîne de blocs, mais celle-ci n'est pas entièrement exempte de vulnérabilités, comme les erreurs accidentelles et le piratage. L'automatisation ne garantira pas l'élimination des bogues, des conflits d'intérêts ou de la corruption au sein de la chaîne logistique mondiale.

La chaîne de blocs fonctionne selon un principe de «pseudonymat»: toutes les transactions sont transparentes, mais elles ne sont pas liées explicitement à des personnes ou à des organisations du monde réel, ce qui protège l'identité des parties prenantes à la chaîne d'approvisionnement sans compromettre l'intégrité du registre. La vérification des caractéristiques et des mouvements des biens peut être dissociée de l'identité des utilisateurs, dans la mesure où la chaîne de blocs peut masquer les données sensibles à caractère personnel qui ne sont pas nécessaires à la tenue du registre. Cet anonymat n'est toutefois pas absolu, et, au prix de quelques efforts, il est possible de faire le lien entre des transactions et les parties concernées. Ce mécanisme est largement considéré comme une amélioration du système actuel, mais il pourrait avoir des conséquences en ce qui concerne la vie privée. Une fois que les biens atteignent le consommateur, le suivi détaillé doit s'arrêter ou, du moins, se conformer aux normes en matière de confidentialité et de sécurité des données.

Élaboration d'une politique d'anticipation

La mise en œuvre de la chaîne de blocs dans le cadre de la gestion de la chaîne d'approvisionnement présente des défis réglementaires importants. Des règlements comme la directive européenne sur la publication d'informations non financières pourraient avoir des effets sur le déploiement des chaînes de blocs dans les chaînes logistiques. Cette directive impose aux entreprises de publier des informations fiables sur les aspects sociaux et environnementaux, les questions de personnel, le respect des droits de l'homme et la lutte contre la corruption, en vue de les inciter à davantage de transparence dans leurs opérations. À l'avenir toutefois, l'absence d'intermédiaires à toutes les étapes ou presque de la chaîne logistique pourrait susciter un certain doute chez les parties prenantes, notamment pour ce qui est des formes automatisées d'exécution et de supervision des transactions. Dans la plupart des cas, les notions et les mécanismes de responsabilité en cas d'imprévu doivent non seulement être définies, mais aussi faire l'objet de possibles révisions.

7. Chaîne de blocs et État: repenser les services publics

Dans le contexte de l'ouverture des données, des services et des décisions du secteur public au moyen des technologies numériques, une nouvelle génération de services gouvernementaux en ligne ouverts, responsables, transparents et collaboratifs est en cours d'élaboration. Le conseiller scientifique en chef du gouvernement du Royaume-Uni a récemment publié un rapport qui donne un aperçu des nouveau outils que la technologie de la chaîne de blocs pourrait permettre de créer en vue de réduire la fraude, d'éviter les erreurs, de diminuer les frais de fonctionnement, d'accroître la productivité, d'encourager le respect des règlements et d'imposer la responsabilité dans de nombreux services publics. Les applications possibles concernent la perception des impôts, la gestion de l'identité, le versement des prestations, les monnaies locales ou nationales, les titres de propriété, le cadastre ainsi que toutes sortes d'archives administratives. La même technologie pourrait permettre à des acteurs non gouvernementaux de fournir des services quasi-étatiques, allant du notariat à la création d'une citoyenneté et d'une identité mondiales. Il reste à voir ce que les chaînes de blocs pourront apporter au secteur public.

Comment la technologie de la chaîne de blocs pourrait contribuer aux services publics

Les données utilisées par les institutions publiques sont souvent fragmentées en interne et opaques pour les autres acteurs, notamment les citoyens, les entreprises et les organismes de surveillance. La technologie de la chaîne de blocs pourrait permettre de créer et de vérifier des registres avec davantage de rapidité, de sécurité et de transparence. En effet, l'application la plus directe de cette technologie au sein des administrations publiques concerne la tenue des registres. L'horodatage associé aux signatures numériques sur des registres accessibles devrait offrir des avantages à tous les utilisateurs, en leur permettant de réaliser des transactions et de créer des documents (par exemple des extraits de cadastre, des certificats de naissance ou des permis professionnels) et de réduire la dépendance aux avocats, aux notaires, aux fonctionnaires administratifs ou aux autres tiers.

L'État estonien s'est lancé dans une expérience de mise en œuvre de la chaîne de blocs qui vise à permettre aux citoyens d'utiliser leur carte d'identité pour commander des ordonnances médicales, voter, utiliser des services bancaires, demander des prestations sociales, immatriculer des entreprises, payer des impôts et accéder à environ 3 000 autres services. Le dispositif permet également aux fonctionnaires d'encrypter des documents, d'examiner et d'approuver des permis, des contrats et des demandes ainsi que de soumettre des requêtes à d'autres services. Il s'agit là d'un exemple de chaîne de blocs à permissions, dont une partie de l'accès est restreint afin de préserver les données et de protéger la vie privée des utilisateurs. Qui plus est, le rôle de l'État en tant qu'autorité de contrôle du système contraste avec la structure ascendante de bon nombre d'initiatives prônées par la communauté qui

participe au développement de la chaîne de blocs. Néanmoins, alors que le système est en passe d'être installé chez les notaires et utilisé pour la gestion des dossiers médicaux, il demeure l'une des initiatives de gouvernement les plus avancées en matière d'utilisation de la chaîne de blocs.

Plusieurs pays dont le Ghana, le Kenya et le Nigeria ont commencé à utiliser la chaîne de blocs pour la gestion de leur registre foncier. Ils espèrent ainsi créer un registre de la propriété clair et fiable afin de résoudre les problèmes d'enregistrement, de corruption et d'accès du public aux archives. La Suède mène également des essais visant à consigner les ventes immobilières dans la chaîne de blocs, pour permettre à toutes les parties (banques, État, agent immobilier, vendeur et acheteur) de suivre l'avancée de la transaction à chacune de ses étapes et de garantir l'authenticité et la transparence de la procédure tout en réalisant des économies non négligeables de temps et d'argent.

Le ministère britannique du travail et des retraites a lui aussi fait tester la chaîne de blocs pour le versement des prestations sociales. Dans cette expérience, les citoyens utilisent leur téléphone pour recevoir et dépenser leurs prestations et, avec leur accord, les transactions sont consignées dans un registre distribué. Cette initiative a pour objectif d'aider ces personnes à gérer leurs finances et de créer un système de prestations sociales plus sûr et efficace, d'éviter la fraude et d'améliorer la confiance entre les bénéficiaires et l'État. Le gouvernement britannique étudie également des moyens d'utiliser la technologie de la chaîne de blocs pour suivre l'affectation des fonds octroyés par le gouvernement, des donateurs et des organisations humanitaires ainsi que leur dépense par les bénéficiaires, que ce soit sous la forme de subventions, de prêts ou de bourses d'études.

Incidences et évolutions possibles

L'introduction de la technologie de la chaîne de blocs dans les administrations publiques pourrait aboutir à la rationalisation des procédures internes, à la réduction des frais de transaction, à une confiance accrue envers les interactions et les échanges de données avec d'autres organisations et silos de données étatiques ainsi qu'à une meilleure protection contre les erreurs et les faux. Certaines procédures pourraient par ailleurs être automatisées à l'aide des contrats intelligents. Il convient cependant de tenir compte de certains risques. Premièrement, la migration vers un nouveau système de registre numérique entraîne des frais de mise en service et, durant cette phase de transition, le fonctionnement des systèmes de sauvegarde et de deux systèmes en parallèle pourrait donner lieu à des difficultés techniques et procédurales. De plus, il est important que les attentes en matière de conservation et de contrôle des archives publiques telles que définies lors de la création de ces archives continuent d'être respectées en toutes circonstances. Enfin, étant donné que la technologie ne conserve que des condensés (décrits dans la partie sur les brevets) ou d'autres représentations numériques incomplètes des documents, les personnes et les organisations privées devront allouer davantage de ressources à la conservation des documents à long terme.

La chaîne de blocs permet de consigner l'horodatage et les détails d'une transaction, mais elle n'offre pas la possibilité de vérifier l'exactitude de ce que contient cette transaction. Tant que la transaction répond aux exigences techniques du protocole, elle devient une entrée immuable dans le registre, quelle que soit la véracité de son contenu. De la même manière que toutes les demandes et les soumissions d'informations à la fonction publique sont examinées avant d'être acceptées, il convient de garantir un examen adéquat lors de l'acceptation et du partage d'informations sur la chaîne de blocs correspondante. Même s'il sera éventuellement possible un jour de permettre l'automatisation de certaines de ces procédures et de les sécuriser, elles ne sauraient remplacer les les fonctionnaires dans leur rôle de garde-fou.

L'immuabilité des données de la chaîne de blocs, qui signifie qu'elles ne peuvent pas être altérées ou effacées une fois consignées, instaure la transparence et la responsabilité. Cependant, elle pourrait également compromettre la confidentialité et la protection des données, en particulier lorsqu'il est question de données à caractère personnel ou sensible, qui ne devraient jamais être stockées dans la

chaîne de blocs. La chaîne ne garantit pas l'anonymat, et plus les données sont personnelles, plus il est aisé d'identifier la personne à laquelle elles appartiennent. Cette immuabilité pourrait mettre en péril le droit à l'oubli, en vertu duquel les utilisateurs peuvent, sous certaines conditions, demander que leurs données personnelles soient effacées.

Il est important de garantir l'accès de tous les citoyens aux services publics. La chaîne de blocs risque bien de creuser le fossé numérique existant. Les citoyens qui n'ont pas accès à internet pour une quelconque raison pourraient ne pas être en mesure de jouir pleinement et directement des avantages qu'offrent les avancées liées aux chaînes de blocs pour ce qui est du renforcement de leur contrôle sur leurs propres données et transactions. Souvent, les services fondés sur la chaîne de blocs resteront cachés sous des interfaces familières et conviviales. Les modalités précises de la mise en œuvre du protocole relativement à sa structure et à son interface d'utilisation présentent une grande importance sur le plan des valeurs politiques et sociales prônées par le système. Enfin, il convient de remarquer que certaines initiatives favorisent le contournement des institutions et des autorités traditionnelles et centralisées, y compris des États et des services publics. Des services quasi-étatiques fondés sur la chaîne de blocs et fournis par des acteurs non gouvernementaux font déjà leur apparition. De telles offres pourraient non seulement séduire des communautés de plus en plus numérisées et mondialisées, mais aussi présenter des enjeux complexes pour les pouvoirs publics.

Élaboration d'une politique d'anticipation

Les administrations publiques conserveront probablement un contrôle centralisé important sur la mise en œuvre de leurs chaînes de blocs, et pourraient également demander l'installation de «portes dérobées» dans les systèmes chiffrés privés à des fins d'application de la loi, même si ces mesures pourraient introduire de nouvelles failles de sécurité. Le chiffrement de bout en bout pourrait également être envisagé dans le prochain réexamen de la directive européenne «vie privée et communications électroniques». Les pouvoirs publics pourraient étudier comment la chaîne de blocs peut améliorer les services publics, notamment en insufflant davantage de transparence et de responsabilité, et pourraient choisir de reconnaître ou non les services quasi-étatiques indépendants au sein de leur juridiction.

8. Une chaîne de blocs omniprésente? Les organisations autonomes décentralisées

La vision des premiers pionniers de l'internet était d'instaurer un nouvel ordre social composé d'organisations plus indépendantes, décentralisées et agiles par le truchement de technologies de l'information et de la communication. Certains soutiennent que les modèles fondées sur les communs ou le pair à pair garantissent un meilleur usage des ressources, et d'autres développent déjà des plateformes de coopératives qui sont détenues de manière collective et régies de manière démocratique par leurs utilisateurs ou leurs travailleurs. La chaîne de blocs peut contribuer à de telles organisations en permettant l'échange direct et instantané de données ou de propriété, l'exécution de budgets, l'application automatique de contrats ou la prise de décision au sein des organisations, le tout sous une forme transparente et chiffrée. Cela pourrait-il préfigurer l'émergence de nouvelles organisations reposant sur la chaîne de blocs, et quels en seraient les conséquences pour la société européenne?

Des registres décentralisés pour des organisations décentralisées

Les organisations autonomes décentralisées (Decentralised autonomous organisations ou DAO) peuvent être vues comme un groupe de contrats intelligents formant un jeu de règles de gouvernance qui sont appliquées et exécutées automatiquement au moyen de chaînes de blocs. Une DAO peut jouer le rôle d'un médiateur entre différentes parties au sein d'une organisation certes décentralisée mais sous contrôle humain, ou elle peut constituer une organisation totalement autonome dont le contrôle est entièrement dévolu à des algorithmes. Le degré d'autonomie et d'autosuffisance que les DAO pourront

atteindre reste à établir. La DAO la plus aboutie, connue sous le nom de «The DAO», n'est pas entièrement autonome, mais il n'est pas impossible d'imaginer que d'autres DAO, indépendamment de toute intervention humaine, contrôlent à l'avenir leur propres ressources et interagissent avec d'autres entités humaines et non humaines, y compris d'autres DAO. Par exemple, une DAO pourrait posséder une voiture autonome qui offrirait un service de taxi 24 heures sur 24. Elle dégagerait ainsi un revenu qu'elle utiliserait pour payer son carburant, ses réparations et son assurance, et épargnerait en vue de remplacer le véhicule en fin de vie.

Dans le cadre des DAO, la coopération entre les individus du système et entre les organisations peut s'appuyer non pas sur une autorité centrale ou sur les forces pures du marché, mais sur le consensus cryptographique et la transparence en tant que caractéristiques techniques de base. Les contrats intelligents ancrés dans la chaîne de blocs offrent non seulement la possibilité de conserver un enregistrement inviolable de tous les éléments d'une organisation, mais aussi d'exécuter automatiquement, voire en autonomie totale, des opérations quotidiennes comme l'accès aux biens et aux bâtiments, l'affectation des tâches, la gestion des actions et des droits de vote, la répartition des bénéfices ou la transmission de micropaiements.

Il a été avancé que la chaîne de blocs pourrait donner les moyens à une nouvelle génération d'organisations de changer les rapports économiques et de pouvoir qui structurent les organismes centralisés traditionnels. En voici quelques exemples: une plateforme sociale de partage de contenus multimédias possédée par ses utilisateurs, qui s'évaluent entre eux et sont automatiquement rétribués pour leurs contributions; des applications de covoiturage érigeant les conducteurs en copropriétaires et gestionnaires des activités quotidiennes; ou encore d'autres communautés, comme Steem-it, au sein desquelles les utilisateurs sont également actionnaires et où les bénéfices et les prises de décisions sont partagés de manière transparente.

Incidences et évolutions possibles

La chaîne de blocs peut être utilisée pour élaborer des structures décentralisées à l'intérieur des organisations. Mais, par ailleurs, le recours à la chaîne pour chaque transaction pourrait limiter les flux d'informations qui étaient jusqu'alors principalement libres. La supervision et le contrôle de toute transaction de n'importe quel bien ou contenu pourraient aboutir à des réclamations plus solides au titre du droit à la propriété intellectuelle, par exemple pour la gestion des droits numériques, et pourraient freiner l'innovation et l'émergence de nouveaux acteurs. En s'émancipant du contrôle centralisé, les DAO pourraient éliminer les erreurs et la corruption dues aux humains. Les citoyens tourneront leur confiance, jusqu'ici axée sur la réputation traditionnelle, vers les réseaux techno-sociaux, c'est-à-dire vers les contrats et les devises qui s'appuient sur la chaîne de blocs. Selon certains, ce changement pourrait créer de nouvelles formes d'action démocratique collective en transformant les approches de gouvernance descendante, aujourd'hui critiquées pour leur manque de souplesse, leur opacité, leur lenteur et leur déficit démocratique.

Au cours de la plus importante campagne de financement participatif jamais organisée, The DAO a récolté plus de 100 millions d'euros. Véritable hybride entre un site de financement participatif et un fonds de capital-risque, cette organisation repose sur les contrats intelligents d'Ethereum. Les participants au financement votent pour l'ensemble des décisions, qui vont de la nomination au licenciement des administrateurs en passant par le financement des projets. En juin 2016, une attaque informatique a profité de failles dans le code de cette DAO et siphonné quasiment un tiers de ses actifs, ce qui a suscité une controverse dans la communauté au sujet de la suite des opérations. Les options qui s'offraient alors consistaient à geler les fonds du compte (un «soft fork»), à pirater le système et rétablir les comptes d'origine (un «hard fork») ou à ne rien faire du tout. D'une part, étant donné que le ou les attaquants avaient profité d'une faille dans le code informatique, il pouvait être considéré que le contrat n'avait pas été rompu et qu'une modification de la chaîne de blocs de The DAO porterait atteinte à la confiance du public à l'égard de son caractère immuable. D'autre part, l'attaque allait clairement à

l'encontre de l'esprit du contrat, constituait une violation potentielle du droit contractuel et pouvait décourager les participants ou ceux qui projetaient de participer à la communauté. Dans tous les cas, l'incident a mis en lumière les failles de sécurité existantes et mis à l'épreuve les fondations idéologiques de la communauté de développement de la chaîne de blocs.

La résistance contre le recours aux structures légales existantes (par exemple, le fait de considérer les développeurs et les mineurs principaux comme des fiduciaires) a suscité des appels en faveur de mécanismes différents ou plus sophistiqués, tels que des systèmes de réputation ou méritocratiques visant à encourager la participation. Certains ont également appelé à l'adoption de normes et de principes éthiques communs. Cependant, les mécanismes autonomes de ces organisations soulèvent également des questions concernant la délégation à des algorithmes et leur rôle réglementaire. Certains soutiennent qu'une gouvernance par le code s'accompagne de devoirs moraux ou d'une responsabilité morale de la part de la communauté lorsqu'il s'agit de prendre des décisions importantes, alors que d'autres travaillent à l'incorporation de valeurs humaines et de la volonté générale des citoyens dans des contrats sociaux algorithmiques.

Élaboration d'une politique d'anticipation

À l'instar de nombreuses initiatives fondées sur la chaîne de blocs, les DAO existent dans une zone floue de la réglementation qui pourrait n'offrir aucune garantie de protection ou de responsabilité, en particulier lorsqu'elles ne s'appuient pas explicitement sur des systèmes juridiques existants. Certaines inquiétudes d'ordre juridique pèsent également sur l'émission d'actions par les cryptoentreprises, démarche qui pourrait les faire relever du cadre existant des marchés de valeurs mobilières et nécessiter qu'elles s'enregistrent et se conforment à divers règlements et obligations. En intervenant en dehors du cadre réglementaire, les organisations fondées sur la chaîne de blocs qui ne sont pas constituées ou reconnues légalement pourraient être victimes d'escroqueries à l'investissement et d'attaques informatiques, et leurs membres pourraient avoir à assumer des responsabilités en tant qu'associés. Certains appellent à davantage de surveillance et de transparence en ce qui concerne la prise de décision algorithmique et la modélisation interactive. La complexité des algorithmes de pointe rend difficile, même pour les développeurs, la pleine compréhension des lois applicables et la vérification de leur respect du droit, par exemple eu égard aux lois anti-discrimination et aux lois sur la transparence. Les organisations autonomes et auto-exécutoires pourraient également remettre en question les notions traditionnelles de personnalité juridique, de libre choix et de responsabilité.

Des DAO pourraient être programmées pour le commerce de produits illicites ou interdits. Même si l'anonymat n'est pas garanti, l'efficacité, l'automatisation et la structure distribuée de la chaîne de blocs sous-jacente pourrait empêcher les instances réglementaires d'appliquer la loi et de mettre fin à de telles opérations. Les victimes d'infractions perpétrées par des DAO pourraient également avoir des difficultés à obtenir des dommages-intérêts ou une injonction à l'encontre de la DAO malveillante dans le cas où la capacité à prendre de telles mesures n'est pas spécifiquement programmée dans sa structure.

Conclusions

L'application de la chaîne de blocs la plus renommée, la plus utilisée et la plus percutante est le bitcoin, mais les retombées potentielles de la technologie sont plus importantes et plus vastes que la simple création de monnaies virtuelles. En effet, étant donné que d'autres applications peuvent s'adosser à la chaîne de blocs du bitcoin, les principales répercussions du bitcoin pourraient survenir en dehors du champ monétaire. Grâce à la chaîne de blocs, les transactions de tous types sont généralement plus rapides et moins coûteuses et elles profitent de la sécurité offerte par le protocole. Si les transactions réalisées en Europe sont souvent rapides, peu coûteuses et suffisamment sécurisées pour la plupart des utilisations, les utilisateurs et les partisans des applications de la chaîne de blocs trouvent souvent des avantages dans sa transparence et son caractère immuable. On observe en effet une tendance à accorder

moins de confiance aux institutions financières et de gouvernance et à nourrir un plus grand nombre d'attentes sociales en matière de responsabilité et d'obligation de rendre des comptes. La popularité de la technologie de la chaîne de blocs pourrait également témoigner de l'émergence d'une tendance sociale qui donne la priorité à la transparence plutôt qu'à l'anonymat.

Bien entendu, à chaque transaction effectuée au moyen d'un registre distribué en lieu et place d'un système centralisé traditionnel, les intermédiaires et les médiateurs sont écartés et perdent leur source habituelle de pouvoir et de revenu. Pour les monnaies, ce sont les banques; pour les brevets, les offices de brevets; pour les élections, les comités électoraux; pour les contrats intelligents, les personnes exécutant les contrats; et pour les services publics, les autorités de l'État. Une croissance significative du taux d'utilisation de la technologie de la chaîne de blocs pourrait changer radicalement la substance, voire le volume du travail des «cols blancs». Par exemple, une partie du travail des intermédiaires et des avocats spécialisés en droit des contrats pourrait être remplacée par des transactions de pair à pair et par des contrats intelligents. De nombreux observateurs ne nourissent aucune inquiétude face à une telle perspective. Certains affirment que seules quelques-unes des tâches les moins intéressantes (comme la fourniture de preuves de certification) seront affectées à la chaîne de blocs, ce qui dégagera du temps pour les tâches essentielles à haute valeur ajoutée, comme la prestation de services sur mesure. Bien que la quantité totale de travail puisse s'en trouvée diminuée, d'autres observateurs citent les similarités qui existent avec les vagues précédentes d'automatisation des postes des «cols bleus» (comme les lignes de production robotisées), où la réaffectation des tâches répétitives avait détruit des emplois tout en créant de nouveaux postes qualifiés dans le domaine de la conception et de la maintenance des systèmes nécessaires. Dans tous les cas, en dépit de la rareté des éléments de preuve, la plupart des observateurs prévoient un changement de la nature des tâches effectuées par les humains mais un maintien du nombre total d'emplois voire même une qualité accrue de ces emplois. Le développement de la chaîne de blocs pourrait également entraîner, de manière indirecte, une augmentation de la consommation d'énergie. En 2014, la consommation d'électricité de la chaîne du bitcoin était comparable à celle de l'Irlande, et ce chiffre n'a fait qu'augmenter depuis. S'il est possible de développer des algorithmes et du matériel plus économes, l'intensité énergétique des chaînes de blocs, et plus largement de tous les processus numériques, pourrait devenir un problème croissant.

L'effet le plus profond du développement de la chaîne de blocs pourrait être lié aux changements subtils dans les valeurs et les structures sociales, changements liés aux valeurs intrinsèques de la technologie. Toutes les technologies sont imprégnées de valeurs et de politiques, qui reflètent généralement les intérêts de leurs créateurs. Ainsi, la raison pour laquelle les systèmes de registre traditionnels placent leurs créateurs à une position d'intermédiaire central apparaît clairement: puisque toutes les transactions doivent passer par eux, les créateurs conservent leur position de pouvoir et la capacité de tirer profit des utilisateurs. Par l'utilisation de technologies, les individus réaffirment les valeurs et les politiques qu'elles représentent. Chaque fois qu'un de ces registres est utilisé pour consigner une transaction, la centralité et le caractère indispensable de l'acteur en son centre sont réaffirmés. À l'évidence, un registre distribué dénué d'intermédiaire central est lui aussi chargé de valeurs et d'orientation politique, car il s'appuie sur la confiance envers les technologies de chiffrement et de mise en réseau et redistribue le pouvoir, jusqu'ici détenu par des autorités centrales, vers des structures de pair à pair non hiérarchisées. Dans ce contexte, le recours à ce type de chaîne de blocs *implique* de s'inscrire dans un mouvement plus large qui vise à réduire la confiance et le pouvoir dévolus aux institutions traditionnelles comme les banques et les gouvernements. Les cas analysés dans le présent document révèlent plusieurs exemples de la façon dont les applications fondées sur la chaîne de blocs incarnent ces valeurs. Bien entendu, pour que ces changements soient perceptibles d'un point de vue social plus général, il faudrait que la chaîne de blocs connaisse un développement considérable, au point de se retrouver d'un bout à l'autre de la vie quotidienne dans les tâches les plus prosaïques.

Élaboration d'une politique d'anticipation

Au premier abord, le caractère décentralisé, chiffré et auto-exécutable des applications technologiques de la chaîne de blocs semble dépendre ou jouer le rôle d'une approche autorégulatrice, qui devrait en principe exister parallèlement aux instruments juridiques traditionnels. Cependant, un examen attentif des applications de pointe met en lumière diverses questions juridiques traditionnelles et nouvelles qu'il convient de prendre en compte de manière contextualisée, étant donné que certaines de ces applications remettent en question des principes fondamentaux du droit et éparpillent l'objet de l'attention des autorités de réglementation, et ce de plusieurs manières.

Tout d'abord, le caractère décentralisé et transfrontalier de la chaîne de blocs soulève des problèmes juridictionnels, compte tenu de l'éparpillement sans précédent des responsabilités institutionnelles et juridiques, ce qui rend l'harmonisation de la réglementation à l'échelle transnationale plus pertinente qu'aux échelles locale ou régionale. Si la technologie de la chaîne de blocs venait à se développer de manière considérable, les structures juridiques centralisées pourraient perdre leur aptitude à contrôler le registre, laquelle serait transférée aux utilisateurs ou à d'autres parties du système, ou leur capacité de façonner l'activité de personnes hétérogènes ou d'organisations autonomes décentralisées, étant donné que personne, ni même son créateur, ne peut exercer de contrôle sur le registre une fois qu'il a été mis en place. Il existera alors moins de points de contrôles susceptibles de guider et de soutenir le flux de données. D'autres problèmes se posent également, comme le caractère exécutoire des contrats intelligents ainsi que les questions de la responsabilité et de l'obligation de rendre des comptes, qui ne peuvent pas pour l'instant être attribuées aux registres distribués, ceux-ci ne disposant de personnalité juridique. Ce problème est exacerbé par leur mode opératoire transfrontalier des contrats intelligents et par le fait qu'ils ne sont pas encore capables de réaliser des opérations complexes.

Les systèmes décentralisés fondés sur la chaîne de blocs pourraient être ouverts à la cooptation par des puissances extérieures et, en l'absence de protection institutionnelle, ces plateformes pourraient se transformer en oligarchies. Si elle s'avérait malveillante, une organisation autonome décentralisée pourrait devenir une source de préoccupations réglementaires au vu du potentiel d'utilisation détournée que présente cette technologie à forte capacité de changement. De plus, les caractéristiques de chiffrement de la technologie de la chaîne de blocs pourraient priver les autorités de toute possibilité de surveillance légale à des fins de poursuites ou d'application de la loi. La protection des consommateurs constituera une autre préoccupation importante des autorités de réglementation, car les clauses contractuelles et les mesures de recours pourraient manquer de clarté pour le consommateur et, du fait de l'automatisation, être difficiles à adapter aux possibles changements de situation. D'autres préoccupations réglementaires portent par ailleurs sur la sécurité, étant donné qu'il est possible de repérer ou de déduire l'identité d'une personne à partir de transactions. Enfin, la chaîne de blocs pourrait soulever des questions en ce qui concerne le choix de la législation et de la juridiction apte à régler les différends.

Il convient de souligner que l'intérêt pour les applications fondées sur la chaîne de blocs semble souvent faire écho à un mécontentement vis-à-vis des systèmes, des procédures et des médiateurs traditionnels. Le développement de la chaîne de blocs présente souvent des similarités avec l'économie du partage, dans la mesure où toutes deux promettent de relier directement les individus, de contourner les intermédiaires et d'éviter, pour la population, un intervention des États, des banques et des autres

institutions importantes, en s'appuyant souvent sur une rhétorique de transition, de dissociation, voire de révolution. Cependant, comme on l'a vu, les initiatives les plus fructueuses de ce mouvement sont devenues une sorte d'intermédiaire ultime, structurellement très éloigné de la vision de décentralisation qu'attendaient de nombreux citoyens. Le même constat pourrait être fait pour la chaîne de blocs, dont les principales retombées surviennent dans des applications qui semblent bien loin de la conception plus idéaliste d'une chaîne décentralisée et transparente. Par exemple, une autorité électorale pourrait mettre en place un système de vote fondé sur une chaîne de blocs à permissions, en conservant le contrôle de la distribution de pseudonymes afin de garantir l'anonymat et en affirmant son rôle d'autorité suprême et de médiateur central par lequel tous les votes doivent passer. Il ne s'agit pas de nier le potentiel technique et les avantages politiques que présente une telle méthode. Au contraire, elle nous rappelle que, dans une telle chaîne à permissions, les degrés de décentralisation et de transparence sont moindres, ce qui a des conséquences sur la structure technique et sur les fonctionnalités du registre, ainsi que sur les valeurs et les politiques qu'il représente. Il est possible d'imaginer des équivalents pour les registres des cadastres, des banques et des offices de brevets, dont chacun pourrait adapter des éléments techniques du protocole de la chaîne de blocs tout en modérant la portée idéaliste des valeurs dont elle est imprégnée. De tels systèmes resteraient probablement susceptibles d'offrir des avantages importants en vue d'une amélioration de la transparence et de la responsabilité et d'une réduction de la corruption. Aussi, en cooptant la chaîne de blocs, les institutions de gouvernance pourraient l'utiliser afin de créer des «technologies de réglementation» dont la mise en œuvre viserait à remplir les mêmes objectifs réglementaires, par exemple de transparence et de responsabilité, que les lois existantes.

Parce que la chaîne de blocs évince les intermédiaires, ceux-ci ne peuvent pas jouer un rôle de régulation quant à son fonctionnement. Ainsi, de nouveaux outils réglementaires doivent être élaborés en vue de faire respecter le droit et de conserver la capacité de planifier et d'agir de manière efficace. En réponse à l'émergence de la technologie de la chaîne de blocs, les institutions de gouvernance pourraient entreprendre quatre grandes catégories d'actions.

- La première option consiste à apporter une réponse aux «problèmes solutionnés par la chaîne de blocs», et ce, sans aucun recours à la chaîne de blocs. Par exemple, si la demande en chaîne de blocs est fondée sur un désir de transparence accrue des procédures, il conviendrait peut-être de garantir aux citoyens un accès élargi aux données et aux procédures publiques sans recourir à la chaîne de blocs.
- Une deuxième option consiste à encourager le développement et l'innovation en matière de chaînes de blocs par le secteur privé en offrant une certaine légitimité à ces produits. Par exemple, sous certaines conditions, des transactions consignées dans la chaîne de blocs pourraient disposer d'une reconnaissance juridique explicite en tant que preuve de l'exécution de transactions.
- Une troisième option est l'inverse de la précédente: décourager tout développement en refusant d'accepter la légitimité des transactions basées sur la chaîne de blocs, par exemple en passant outre ou en annulant des clauses de contrats intelligents.
- La quatrième option consiste à adopter une chaîne de blocs à permissions au sein de systèmes et de structures existants, et à maintenir le rôle et le pouvoir des intermédiaires tout en offrant quelques-unes des fonctions essentielles des chaînes de blocs, mais sans décentralisation ou transparence totale. Ce modèle s'observe déjà dans l'utilisation de la technologie de la chaîne de blocs par le secteur public, par exemple au Royaume-Uni et en Estonie, ainsi que dans le secteur privé.

Des variantes et des combinaisons de ces quatre stratégies pourraient très bien être appliquées à la technologie de la chaîne de blocs dans différents domaines et dans différentes juridictions au cours des dix prochaines années. À l'heure actuelle, il n'existe que peu de demande d'intervention à l'échelle européenne. En effet, un récent rapport du Parlement européen sur les monnaies virtuelles fait état de risques accrus, contre lesquels il conviendra de renforcer les capacités réglementaires, y compris

l'expertise technique, et d'adopter, à l'échelle de l'Union, une approche réglementaire proportionnée, qui ne freine pas l'innovation à un stade aussi précoce.

Notons, enfin, que, si le protocole de la chaîne de blocs prévoit des plateformes permettant des actions positives aussi bien que des actions négatives, cela ne signifie pas pour autant que cette technologie est neutre. Dans sa forme la plus pure, elle favorise la redistribution du pouvoir, jusqu'ici détenu par des acteurs centraux, vers de vastes communautés de pairs. Bien que les ambitions les plus idéalistes et révolutionnaires du développement de la chaîne de blocs demeurent probablement à l'état de projets, une mise en œuvre même modérée de cette technologie pourrait encourager un certain degré de redistribution et de transparence. Comme le remarque Leda Glyptis, la chaîne de blocs ne rendra pas les gens meilleurs, mais elle pourrait rendre certaines des précautions nécessaires à leur vie quotidienne plus rapides, moins coûteuses, plus sûres et plus transparentes.

La technologie de la chaîne de blocs suscite l'intérêt grandissant des citoyens, des entreprises et des législateurs à travers l'Union européenne. La présente analyse vise à informer, de manière accessible, les personnes qui s'intéressent à cette technologie, afin de susciter la curiosité et de donner lieu à des discussions au sujet de ses retombées potentielles. Après une introduction d'ordre général, l'analyse aborde plus en détail huit domaines dans lesquels la chaîne de blocs est susceptible d'avoir des incidences importantes. Les parties relatives à chacun de ces domaines décrivent les applications possibles de cette technologie, les incidences potentielles et les enjeux à anticiper en matière de politique.

Étude publiée par la
Direction de l'évaluation de l'impact et de la valeur ajoutée européenne
Direction générale des services de recherche parlementaire, Parlement européen

PE 581.948
ISBN 978-92-846-1043-3
doi: 10.2861/722047
QA-02-17-043-FR-N