L'IMPACT DES BLOCKCHAINS sur les droits de l'homme, la démocratie et l'État de droit

Service de la société de l'information

DGI(2022)06

Auteurs :
Florence G'sell
Florian Martin-Bariteau

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Edition anglaise :
The Impact of Blockchains for Human Rights, Democracy, and the Rule of Law

Couverture et mise en page :
Service de la société de l'information
Conseil de l'Europe

Images : Shutterstock

Cette publication n'a pas fait l'objet d'une relecture typographique et grammaticale de l'Unité éditoriale du SPDP.

L'IMPACT DES BLOCKCHAINS sur les droits de l'homme, la démocratie et l'État de droit

Aperçu d'ensemble

Rapport rédigé pour le Conseil de l'Europe par

Florence G'sell

Professeure agrégée de droit privé, Université de Lorraine

Titulaire de la Chaire Digital, Gouvernance et Souveraineté de Sciences Po (École d'affaires publiques)

Florian Martin-Bariteau

Professeur agrégé en droit et titulaire de la Chaire de recherche de l'Université en technologie et société, Université d'Ottawa

Conseil de l'Europe

Table des matières

Résumé **3**

Introduction **4**

1. Éléments de base sur les blockchains **6**

Qu'est-ce qu'une blockchain ? *6*

Crypto-monnaies *9*

Contrats « intelligents » ("smart" contracts) *10*

Organisations autonomes décentralisées (DAO) *13*

Jetons non fongibles (NFT) *15*

Critiques suscitées par les blockchains *16*

2. Opportunités pour les droits de l'homme et la démocratie **19**

Améliorer l'exercice des libertés grâce au pseudo-anonymat *19*

Avantages du pseudo-anonymat pour les libertés fondamentales 20

Limites du pseudo-anonymat 20

Renforcer l'anonymat sur les blockchains 21

Gérer des identités numériques *22*

Le contrôle de l'identification : la notion d'« identité autonome » (SSI) 23

Permettre l'autodétermination informationnelle *25*

Soutien aux réfugiés et aux populations vulnérables *27*

Fournir une identité aux réfugiés 27

Lutte contre la traite des êtres humains, notamment des enfants 27

Gérer et distribuer les aides et les ressources 28

Soutenir les personnes dépourvues de compte bancaire 29

Assurer le respect des droits des travailleurs 29

Limites et effets pervers du recours à la blockchain 29

Lutter contre les atteintes aux droits de l'homme sur les chaînes d'approvisionnement *30*

Protéger les titres fonciers et la propriété immobilière *32*

Permettre l'exercice du droit de vote et la transparence démocratique *32*

Fournir des solutions de règlement des litiges *34*

3. Questions juridiques soulevées par les technologies distribuées 36

Risques en matière de protection des données personnelles 36

Conflits de lois et de juridictions 38

« Contrats » intelligents (smart "contracts") 39

Nature juridique 39

Automatisation et immutabilité 40

Encodage des termes juridiques et interprétation du code informatique 41

Mise en œuvre et exécution 42

Limites nécessaires 43

Nature juridique des organisations autonomes décentralisées 43

Conclusion 46

Annexe — Blockchain et Convention européenne des droits de l'homme 48

Résumé

La technologie blockchain offre aux pouvoirs publics, aux organisations internationales, aux ONG, aux entreprises et, de manière générale, au grand public le moyen d'œuvrer à un meilleur respect des droits de l'homme et répondre à certains enjeux.

Après des années durant lesquelles cryptographes et ingénieurs réseau ont œuvré au développement de la technologie, c'est le 31 octobre 2008 que Satoshi Nakamoto a, dans un « livre blanc », présenté un premier projet de blockchain conçu pour constituer un véritable système financier fondé sur une crypto-monnaie, le Bitcoin. Si le Bitcoin fut la première, il existe aujourd'hui plus de 18 000 crypto-monnaies. En outre, bien que la blockchain soit le plus souvent associée aux crypto-monnaies et aux différents instruments ou actifs financiers, elle permet également des usages ou fonctions variés grâce aux applications décentralisées et aux *smart contracts* (« contrats intelligents »). On retrouve ainsi des blockchains dans une foule de domaines tels que la gestion des identités numériques, des dossiers médicaux, des titres et registres fonciers, des droits de propriété intellectuelle, des systèmes de vote en ligne, des chaînes d'approvisionnement, etc.

Le présent rapport étudie les avantages et les risques potentiels de la technologie blockchain pour la démocratie, les droits de l'homme et l'État de droit. À partir de l'étude de plusieurs exemples d'applications fondées sur la blockchain, ce rapport formule, à l'intention du Conseil de l'Europe, une première série de recommandations relatives aux recherches devant être menées dans ce domaine à l'avenir et aux axes de réflexion devant être privilégiés.

Le rapport met en évidence les caractéristiques les plus prometteuses de la blockchain et de ses applications, telles les crypto-monnaies, les *smart contracts*, les organisations autonomes décentralisées (DAO) ou les jetons non fongibles (NFT). L'étude présente aussi les limites de la technologie, qui sont non négligeables et font peser un risque d'atteinte aux droits fondamentaux.

Beaucoup d'applications de la technologie blockchain peuvent servir les objectifs du Conseil de l'Europe, car elles permettent de mieux protéger la démocratie et défendre les droits de l'homme, en alliant responsabilité et transparence. Le rapport présente donc plusieurs exemples d'usages de la blockchain allant en ce sens comme la gestion autonome des identités numériques, la protection des données des individus, l'aide aux réfugiés et aux populations vulnérables, le contrôle des chaînes d'approvisionnement, l'enregistrement des titres fonciers, l'organisation de vote en ligne et les systèmes de règlement des litiges en ligne.

Dans le même temps, le rapport examine certains des problèmes juridiques que pourraient poser les usages de cette technologie. Il met l'accent sur les aspects de la technologie qui pourraient justifier une prise de position du Conseil de l'Europe : protection de l'anonymat et de la vie privée, statut juridique des contrats automatisés et des DAO, conflits de lois et de juridictions résultant de l'architecture transnationale et distribuée des blockchains.

Enfin, le rapport comporte en annexe un tableau présentant les bénéfices et les risques de la technologie blockchain à la lumière des dispositions de la Convention européenne des droits de l'homme.

Introduction

Il est rare que l'invention d'une technologie nouvelle vise à résoudre des problèmes anciens, qu'ils soient sociaux, économiques ou politiques. Telle est pourtant l'ambition de la technologie blockchain, développée dès l'origine dans l'objectif de surmonter enfin les traditionnels problèmes de coopération et de coordination présents au sein des organisations et des communautés humaines. L'idée est de remplacer les institutions établies, telles les banques ou les États, par des outils technologiques et impartiaux capables de susciter la confiance en dehors des cadres habituels — en supprimant ainsi le besoin de tiers de confiance. Le principe fondateur de la technologie blockchain est d'offrir à tous ceux qui le souhaitent la possibilité d'interagir en ligne sur une plateforme régie par le code informatique, qui n'est ni contrôlée ni administrée par une quelconque autorité humaine. La possibilité pour les utilisateurs d'effectuer des transactions pair-à-pair en ligne, sans intermédiaire ni intervention d'un tiers de confiance, limite les risques d'erreur humaine ou de corruption.

L'idéologie qui sous-tend cette technologie a été clairement exprimée en 1992 par Timothy C. May dans son *Manifeste crypto-anarchiste*. Synthétisant des années de discussions en ligne au sein de la communauté cryptographique, ce manifeste prédisait et appelait de ses vœux de nouvelles techniques cryptographiques permettant aux individus et aux groupes de communiquer et d'interagir en ligne de manière anonyme. Par-dessus tout, les crypto-anarchistes souhaitaient permettre aux individus de vivre, communiquer et échanger sans être surveillés, contrôlés ou taxés par les États. Le projet crypto-anarchiste d'une plateforme totalement décentralisée pouvait ainsi permettre de renouer avec l'architecture initiale d'Internet, depuis lors battu en brèche par l'apparition d'immenses plateformes commerciales centralisées.

Des années plus tard, la croyance libertarienne selon laquelle le chiffrement et les outils cryptographiques pourraient libérer les masses est toujours bien vivante. En combinant cryptographie et architecture distribuée, les blockchains sont conçues pour fournir l'infrastructure technologique nécessaire aux interactions humaines de nature sociale, politique ou économique, sans l'intervention de tiers de confiance. Dans le même temps, la primauté accordée au code informatique sur tout autre type de contrainte peut laisser penser que les communautés humaines interagissant sur les plateformes blockchain n'ont plus besoin du droit. Cela explique sans doute pourquoi les juristes qui étudient la technologie blockchain commencent généralement par se demander si les règles juridiques qu'ils connaissent peuvent s'appliquer dans un environnement précisément conçu pour favoriser la programmation au détriment des règles humaines. Telle sera également la perspective de ce rapport, principalement consacré à la question de savoir si et dans quelle mesure les droits fondamentaux des personnes qui interagissent sur les blockchains sont menacés ou garantis.

À ce jour, la blockchain est surtout associée aux crypto-monnaies et aux instruments ou actifs financiers. Sa première application, la blockchain Bitcoin, a consisté en la création d'une monnaie virtuelle et d'un système financier. Depuis le lancement de Bitcoin, en 2008, les blockchains se sont tellement multipliées et ont impliqué des montants si importants que les médias publient régulièrement des histoires racontant l'engouement économique autour des crypto-actifs, ou l'utilisation de ceux-ci par des acteurs malfaisants. Cependant, la technologie blockchain permet des applications allant bien au-delà des seules crypto-monnaies. Certaines permettent, précisément, de protéger effectivement les droits de l'homme. En effet, la technologie blockchain s'est appuyée sur des années de recherche en informatique pour créer des systèmes sécurisés et immuables. L'objectif de ce rapport est donc d'étudier non pas les risques financiers suscités par cette technologie, mais les avantages potentiels et les risques de la blockchain pour la démocratie, les droits de l'homme et l'État de droit.

Ce rapport commence donc par brièvement présenter la technologie blockchain et ses diverses applications, des crypto-monnaies aux *smart contracts* en passant par les organisations autonomes décentralisées (DAO, pour *Distributed Autonomous Organizations*) et les jetons non fongibles (NFT, pour *Non-Fungible Tokens*). Il expose ensuite différentes possibilités d'utilisation de la technologie permettant de renforcer la protection des droits fondamentaux, en ligne avec les objectifs poursuivis par le Conseil de l'Europe. Le rapport aborde ensuite les difficultés juridiques posées par la technologie qui justifieraient une réflexion plus approfondie de la part du Conseil de l'Europe. Enfin, comme il s'agit d'un premier rapport qui vise à présenter des cas d'utilisation et à signaler les problèmes potentiels, l'étude se termine par des recommandations comprenant des pistes de recherches recherches futures et des actions envisageables pour le Conseil de l'Europe. Un tableau résumant les opportunités et les risques de la technologie blockchain du point de vue des dispositions de la *Convention de sauvegarde des droits de l'homme et des libertés fondamentales* (« *Convention européenne des droits de l'homme* ») est fourni en annexe.

Il convient de noter que les questions juridiques relatives aux crypto-monnaies et aux crypto-actifs (c'est-à-dire lorsque les jetons sont utilisés comme moyens de paiement, titres financiers ou autres types d'actifs) sortent du cadre du présent rapport et ont fait l'objet d'autres études. En effet, le Comité d'experts du Conseil de l'Europe sur l'évaluation des mesures de lutte contre le blanchiment d'argent et le financement du terrorisme a examiné de manière approfondie les questions de blanchiment d'argent et de financement d'activités illicites propres aux crypto-monnaies.

De même, le rapport ne traitera pas des activités criminelles impliquant la technologie blockchain. Certes, l'engouement pour la blockchain a entraîné une augmentation de telles activités, notamment par l'utilisation de crypto-monnaies pour les rançons et les paiements illicites. Cependant, d'un point de vue juridique, les infractions elles-mêmes ne sont pas propres à la technologie. La plupart des pays ont désormais mis à jour leurs législations afin de garantir la licéité des transactions, en imposant notamment des règles de conformité obligeant à la connaissance du client (KYC pour *Know Your Customer/Client*). En outre, les services de police peuvent exploiter la transparence totale des registres. Cela étant dit, le pseudo-anonymat et la nature globale et distribuée des blockchains peuvent présenter des défis importants pour les autorités répressives et seront discutés.

Références

Cheng, Evelyn (2017), Dark web finds bitcoin increasingly more of a problem that a help, tries other digital currencies.

Crumpler, William (2021), The Human Rights Risks and Opportunities in Blockchain, CSIS.

De Filippi, Primavera & Aaron Wright (2018), *Blockchain and the Law : The Rule of Code*, Harvard University Press.

May, Timothy (1988), The Crypto Anarchist Manifesto.

Rueckert, Christian (2019), Cryptocurrencies and fundamental rights, *Journal of Cybersecurity*, 5 : 1.

Weinstein, Jason (2021), Why Bitcoin is Better for Crime Fighters than Criminals.

Werbach, Kevin (2018), *The Blockchain and the New Architecture of Trust*, MIT Press.

1. Éléments de base sur les blockchains

Cette section présente la technologie blockchain, notamment son mode de fonctionnement, ses limites et les types d'applications possibles. Pour les besoins de ce rapport non technique, la présentation peut parfois être simplifiée afin de rendre compréhensibles des aspects techniques clés dans un langage accessible, de manière à dépasser, dans la perspective de recherches à venir, l'habituelle présentation médiatique et à reconnaître le potentiel de la technologie tout en clarifiant ses limites.

Qu'est-ce qu'une blockchain ?

Après des années de recherches menées par des cryptographes et des ingénieurs réseaux, la technologie a été présentée par Satoshi Nakamoto, le 31 octobre 2008, dans le livre blanc de la crypto-monnaie Bitcoin. Derrière le pseudonyme de Satoshi Nakamoto se trouvent un ou plusieurs chercheurs anonymes qui ont voulu proposer une solution sécurisée permettant d'effectuer un certain nombre d'opérations, comme le transfert et le stockage de valeurs ou de données, sans l'intervention d'un tiers de confiance.

Les blockchains sont des systèmes de registre distribués et sécurisés qui peuvent fonctionner de manière autonome sans avoir besoin d'une autorité centrale de contrôle ou de coordination, ce qui permet de se passer de confiance et d'intermédiaires. Ces systèmes permettent de réaliser diverses opérations, comme des transferts de valeur ou d'informations, sans aucune intervention d'un tiers de confiance. Cet aspect de la technologie blockchain, qui consiste à rendre l'information sécurisée et quasi-immuable sans avoir besoin d'un tiers de confiance, présente un intérêt essentiel dans le domaine humanitaire ou du point de vue de la défense de la démocratie, notamment dans les cas où les organisations gouvernementales et non gouvernementales peuvent ne pas avoir la confiance du public ou ne pas se faire confiance entre elles.

Une blockchain stocke les données de façon séquentielle, dans un registre qui est répliqué et synchronisé au sein d'un réseau de nœuds distribués, protégé par plusieurs couches de sécurité, depuis la manière dont les blocs sont reliés entre eux jusqu'à la redondance et la synchronisation du réseau. La transparence est une caractéristique essentielle des blockchains qui sont des registres entièrement publics : tout utilisateur est en mesure de lire les informations du registre, ainsi que d'y inscrire de nouvelles informations sous réserve de respecter le protocole de consensus.

Bien qu'elle ne soit pas entièrement dépourvue de failles, la technologie présente d'importantes garanties de sécurité pour l'intégrité des données et la tenue d'archives. Elle permet de s'assurer qu'aucune partie ne peut altérer les informations contenues dans le registre. Chaque fois qu'un bloc de données est ajouté au registre, il comprend une empreinte unique (appelée hachage) des données précédentes contenues dans le bloc précédent. Le registre est formé par une chaîne de blocs qui s'ajoutent les uns aux autres. Il s'agit d'une première couche d'immutabilité, car un bloc donné ne peut être modifié sans altérer tous les blocs suivants. Si un bloc de données est modifié, le hachage de ce bloc change et ne correspondra pas au hachage stocké dans le bloc suivant. Si cela se produit, tous les blocs suivants seront automatiquement écartés.

Les données stockées sont en outre protégées par leur reproduction au sein d'un réseau pair-à-pair distribué qui permet d'éliminer les risques inhérents aux bases de données centralisées. Si quelqu'un tente d'altérer les informations stockées sur la blockchain, le protocole du réseau

distribué permet de le détecter et de l'empêcher. En effet, chaque nœud du réseau possède une copie complète du registre. Donc si un nœud est altéré, seule sa copie du registre sera affectée, et non pas la copie des autres nœuds. Dans un réseau distribué, si un nœud est défaillant, le réseau continue de fonctionner sans perte de données ou d'intégrité. Cela permet de résister aux pannes et aux attaques, car le réseau et le registre ne sont pas compromis lorsqu'un ou quelques nœuds connaissent des difficultés. Il est même possible que le reste du réseau ne s'aperçoive pas de l'anomalie.

La blockchain, en tant que registre distribué, est mise à jour et synchronisée de manière sécurisée selon les procédures définies dans l'algorithme de consensus, qui vise à éviter toute situation dans laquelle la falsification d'un nœud compromettrait le reste du réseau. Les nœuds du réseau distribué assurent chacun la mise à jour de leur copie du registre à partir des informations qui leur parviennent quant aux transactions qui ont été effectuées. Ces transactions sont vérifiées, validées et rassemblées dans des blocs, qui sont ajoutés par les nœuds à leur copie du registre lorsqu'ils sont certains que ces blocs sont valides. Pour faire en sorte que la plupart des nœuds détiennent une même version du registre, il convient que les nœuds parviennent à un consensus sur la validité des blocs de transactions. Dans ce cadre, ce sont les opérateurs de nœuds, les « mineurs », qui ont la responsabilité de valider et de certifier toutes les opérations et tous les blocs de transaction. Une fois qu'un bloc est validé et diffusé, les nœuds le vérifient et l'ajoutent à leur copie du registre ou le rejettent. C'est ainsi que les nouveaux blocs sont ajoutés au registre. Il reste que les différentes blockchains ont des méthodes de validation des blocs qui varient. La plus courante, que l'on retrouve dans la blockchain Bitcoin, est la méthode de « preuve de travail » (*proof of work*), qui consiste à effectuer des calculs cryptographiques complexes pour résoudre un problème mathématique nécessitant une puissance de calcul importante. Cette méthode peut être coûteuse en termes d'énergie. Elle conduit à une compétition entre les mineurs pour résoudre les calculs plus rapidement que les autres, car ils sont ensuite récompensés par des jetons lors de la confirmation du bloc. Or cette compétition augmente continuellement le besoin de puissance de calcul et d'énergie.

En réponse, d'autres mécanismes de consensus ont été développés, la principale alternative étant la « preuve de participation » (*proof of stake*). Au lieu de confirmer les blocs au moyen de calculs très énergivores, il s'agit d'attribuer le pouvoir de minage soit en fonction du nombre de jetons détenus, soit au hasard parmi les mineurs qui détiennent une participation minimum. Cette méthode est plus économe en énergie. Une autre méthode utilise la « preuve de stockage » (*proof of space*), qui consiste à attribuer le pouvoir de minage en fonction de la puissance de calcul ou de l'espace de stockage dont dispose chaque mineur. Cependant, cette méthode favorise moins les économies d'énergie, car elle récompense toujours la puissance de calcul ou de stockage d'un mineur.

Le réseau peut parfois présenter des incohérences. Quand c'est le cas, la version qui figure dans la majorité des nœuds l'emporte et tout le réseau est mis à jour en conséquence. La version minoritaire est déplacée dans une chaîne latérale. Cette couche supplémentaire de sécurité, obtenue grâce à la règle majoritaire, est aussi l'un des points faibles de la technologie. Une blockchain n'est sûre que si la puissance est équitablement répartie entre les opérateurs des nœuds. Toute concentration de pouvoir menace la sécurité de l'ensemble du réseau. Dès qu'un acteur ou groupe d'acteurs contrôle 51 % du réseau, il a le pouvoir de prendre le contrôle de l'ensemble du réseau et d'exclure ou de modifier intentionnellement des transactions. Cette menace pour la sécurité, appelée « attaque des 51 % », explique pourquoi les opérateurs surveillent de près les coalitions et les regroupements de nœuds, notamment en géolocalisant les opérations. Ce risque pour la sécurité est néanmoins minime pour les réseaux établis

comportant un grand nombre de nœuds, car les coûts encourus par un acteur tiers pour se lancer dans une telle attaque seraient astronomiques.

Parmi les avantages de la blockchain figurent aussi **la transparence et le pseudo-anonymat**. Les blockchains sont des registres publics et transparents. Chaque nœud possède une copie complète du registre, et il est possible à tout intéressé de lire toutes les informations enregistrées et de tracer toutes les transactions et opérations effectuées. Il n'est pas possible de dissimuler ou falsifier des informations sur une blockchain, sauf si les informations stockées sont cryptées par les utilisateurs.

Cependant, malgré cette transparence, l'identité des parties est dissimulée grâce à la pseudo-anonymisation. Les nœuds et les utilisateurs n'ont pas besoin de fournir leur nom ou des détails personnels pour interagir sur le réseau. Chaque utilisateur se voit attribuer une clé publique et une clé privée — la clé publique est une adresse connue de tous, et la clé privée n'est connue que de son propriétaire à des fins d'authentification, pour signer ses messages et déchiffrer les messages adressés à son adresse publique. Les utilisateurs sont connus sous leur adresse publique plutôt que sous leur nom. Il est donc impossible de savoir qui se cache derrière une adresse publique donnée, en tout cas lorsqu'aucune information n'a été divulguée quant à l'identité de l'utilisateur au moment de la création de l'adresse. Les utilisateurs peuvent d'ailleurs avoir plusieurs adresses.

Néanmoins, et contrairement aux idées reçues, les blockchains ne permettent pas un anonymat total. Il reste possible de ré-identifier le détenteur d'une adresse puisqu'il est possible de retracer toutes ses transactions et d'en déduire l'identité de l'utilisateur. Certaines transactions sont liées à des actifs du monde extérieur (*off chain*) dont le propriétaire est connu ; certains schémas d'opérations peuvent révéler des communautés ou des comportements dans le monde réel. Un utilisateur peut également fournir son adresse publique à un tiers qui connaît son identité. L'analyse des transactions sur et hors de la chaîne par des enquêteurs peut prendre du temps, mais elle peut permettre de dévoiler l'identité d'un utilisateur, ainsi que l'historique complet de ses opérations. Les services de police se sont servis de ces techniques pour déterminer l'identité de criminels et suivre leurs activités sur et en dehors des blockchains.

Dans certains contextes, la transparence du registre peut être problématique. En effet, l'accès public aux informations et la possibilité de suivre les données et les utilisateurs peuvent présenter des risques pour la vie privée ou la confidentialité. Pour surmonter ce risque, des protocoles et des solutions de protection de la vie privée sont en cours de développement. (Ces considérations relatives au respect de la vie privée seront examinées en détail ci-dessous, dans la section 3). De même, le fait que cette technologie soit ouverte à tous peut poser problème pour certains usages.

En réponse, des alternatives à la technologie des blockchains publiques et ouvertes ont été proposées, avec des blockchains hybrides à permission dans lesquelles les utilisateurs se voient délivrer des autorisations spécifiques pour effectuer certaines activités sur le réseau. Les possibilités peuvent aller d'un accès public en lecture seule à un accès contrôlé en écriture, voire à des schémas d'autorisation plus complexes. Il est également possible de créer des blockchains entièrement privées, accessibles au sein d'une organisation ou d'un consortium d'organisations, où le fonctionnement de la blockchain et l'accès aux données peuvent être limités à un petit nombre d'utilisateurs approuvés.

Enfin, l'une des principales caractéristiques des blockchains est leur fonctionnement automatisé et leur fiabilité. Les processus d'exploitation et de vérification s'exécutent de manière autonome chaque fois qu'un nœud prend connaissance des informations disponibles, tout en vérifiant l'intégrité de la chaîne. Il n'y a aucune marge de manœuvre pour les parties — lorsqu'une information, une transaction, un ordre est ajouté au registre, il sera transmis et

exécuté à travers le réseau automatiquement. Cela présente une série d'avantages majeurs en cas de manque de confiance entre les parties, puisque l'on peut se passer ici d'intermédiaires pour exécuter les opérations et faire respecter les règles.

Références

Bacon, Jean, Johan David Michels, Christopher Millard & Jatinder Singh (2018), Blockchain Demystefied: A Technical and Legal Introduction to Distributed and Centralised Ledgers, *Richmond Journal of Law & Technology* 25 : 1.

Narayanan, Arvin, Joseph Bonneau, Edward Felten, Andrew Miller & Steven Goldfeder (2016), *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press.

Nakamoto, Satoshi (2008), Bitcoin: A Peer-to-Peer Electronic Cash System.

Walch, Angela (2015), The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk, *NYU Journal of Legislation and Public Policy* 18 : 837.

Crypto-monnaies

Une crypto-monnaie est une forme de monnaie virtuelle utilisant la technologie blockchain. La première crypto-monnaie pleinement fonctionnelle, le Bitcoin, a été proposée en 2008 et lancée en 2009. La crise financière mondiale qui sévissait à l'époque avait affecté la confiance dans le contrôle exercé par les institutions financières existantes, ainsi que dans la capacité des États à assurer une surveillance adéquate. Dans un texte fondateur, *Bitcoin : A Peer-to-Peer Electronic Cash System* (« Bitcoin : un système de paiement électronique pair-à-pair »), le mystérieux Satoshi Nakamoto a présenté le projet de plateforme « Bitcoin », un système de paiement distribué, purement pair-à-pair et totalement dépourvu d'intermédiaires. Le Bitcoin a été conçu pour faciliter les transferts de fonds en ligne directement entre parties afin de supprimer le besoin d'autorité centrale et de tiers de confiance ainsi que les coûts correspondants.

La nature décentralisée de la blockchain, et par extension du Bitcoin, est l'un des fondements du système. Pour construire un système financier distribué, le principal problème technique relevait de la mise en place d'un protocole de consensus distribué. Les utilisateurs disposent de portefeuilles cryptographiques, qui font office de comptes, et peuvent directement transférer et recevoir des fonds, sous réserve de validation par les utilisateurs du système. Tout l'historique des transactions est disponible sur le registre public, bien que l'identité du propriétaire du portefeuille reste protégée par le pseudonymat.

Quand A veut transférer des Bitcoins à B, la transaction entre les portefeuilles électroniques A et B est signée et diffusée à tous les nœuds de la blockchain. Les mineurs confirment la disponibilité des fonds et parviennent à un consensus, sur toute la blockchain, sur le fait que le transfert a eu lieu et que la quantité de bitcoins voulue a changé de propriétaire. B peut vérifier la transaction sur le registre et confirmer que le transfert sur son portefeuille s'est bien produit. La nature ouverte du registre vise à assurer la transparence et à éviter les doubles dépenses. En plus de créer une monnaie virtuelle et un système de paiement, la blockchain Bitcoin prévoit sa propre politique monétaire. Au cours du processus de minage, de nouvelles unités de crypto-monnaie sont créées pour récompenser les mineurs qui valident les blocs et les ajoutent au registre.

Le Bitcoin a attiré et ne cesse d'attirer une foule d'adeptes et de sous-produits, mais ce n'est pas — et de loin — la seule crypto-monnaie en circulation aujourd'hui. Il en existe plus de

18 000. Plusieurs d'entre elles, dans le sillage du Bitcoin, sont conçues pour permettre des paiements et des transferts d'argent entre utilisateurs en préservant la vie privée, comme Litecoin ou Monero. Chaque crypto-monnaie a sa propre politique monétaire. Pour certaines, leur valeur est liée à la demande sur le marché tandis que d'autres, comme le Tether, sont adossées à une monnaie fiat pour plus de stabilité. D'autres encore ont été créées pour plaisanter, comme le Dogecoin, créé à partir d'un mème représentant un chien Shiba Inu : il s'agissait de tourner en dérision le côté fortement spéculatif des crypto-monnaies…

De même, certaines monnaies ont été développées pour des usages et des fonctions spécifiques. Il convient de noter que, malgré leur nom, toutes les crypto-monnaies ne sont pas utilisées comme monnaies. Si certaines sont utilisées comme actifs ou instruments financiers, les jetons peuvent servir à de nombreux autres usages. Par exemple, la blockchain Namecoin fournit un service décentralisé de système de noms de domaine (DNS) pour les adresses Internet sous l'extension .bit, qui échappe à la censure. De même, le jeton Storj permet aux utilisateurs de partager des fichiers sur un réseau décentralisé.

Plus d'une décennie après sa création, la technologie blockchain remplit de nombreuses autres fonctions, notamment grâce à des blockchains comme Ethereum ou Cardano, qui servent de support à des applications décentralisées et des « contrats intelligents » (*smart contracts*). Sur ces plateformes, les développeurs peuvent déployer des systèmes permettant de gérer une foule de services, de l'identité numérique aux dossiers médicaux, en passant par les titres fonciers et les plans d'occupation des sols, les droits de propriété intellectuelle, les systèmes de vote, les chaînes d'approvisionnement ou l'aide internationale.

Références

Nakamoto, Satoshi (2008), Bitcoin : A Peer-to-Peer Electronic Cash System, traduction française par Arnaud-François Fausse, Bitcoin : un système de paiment électronique pair-à-pair.

Narayanan, Arvin, Joseph Bonneau, Edward Felten, Andrew Miller & Steven Goldfeder (2016), *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press.

Contrats « intelligents » (“smart” contracts)

En 2014, Ethereum a lancé une nouvelle blockchain permettant non seulement le transfert de jetons de crypto-monnaie (appelés ethers), mais aussi le développement d'applications appelées, de manière trompeuse, *smart contracts*. Malgré leur nom, il faut souligner que ces « contrats intelligents » ne sont pas, à proprement parler, des contrats au sens juridique du terme.

Un *smart contract* est un protocole informatique qui prévoit l'exécution automatique de certaines tâches ou opérations lorsque certaines conditions sont réunies. Les « clauses » codées en langage informatique s'exécutent automatiquement lorsque les conditions prévues par le programme surviennent, sans aucune intervention humaine. Les instructions codées sont déclenchées par certains événements. En coulisse, une série d'instructions de type « si… alors » déclenche les actions : si la condition X se réalise, alors l'action Y se produit automatiquement. C'est à la fois très simple et très puissant. Comme pour tout logiciel, les possibilités sont illimitées, à condition que les instructions puissent être exprimées en code informatique et qu'une machine puisse mettre en œuvre l'action voulue. Les *smart contracts* présentent, entre autres, le grand avantage de supprimer le recours à des tiers et les risques liés à la marge de manœuvre dont les parties peuvent disposer. Les *smart contracts* sont à la fois définis par le code informatique et exécutés automatiquement par le code, sans marge d'appréciation.

Les *smart contracts* sont aujourd'hui de plus en plus développés pour tirer parti de la technologie blockchain. Par conséquent, le terme est devenu synonyme de « contrats auto-exécutables sur une blockchain ». Or, les actions automatiques sans (ou presque sans) intervention humaine existaient avant la blockchain. Nick Szabo a théorisé l'idée de *smart contracts* dans ses publications dès le milieu des années 1990. Il a proposé de développer un code informatique clair pour permettre aux ordinateurs d'exécuter des « contrats intelligents » complexes. Ces « contrats » informatisés peuvent être considérés comme « intelligents », car ils peuvent s'auto-exécuter et faire respecter leurs termes — à tout le moins, ils sont plus « intelligents » que les contrats traditionnels qui ne peuvent qu'exprimer l'engagement des parties sans garantir qu'il sera appliqué. Ces programmes informatiques sont jugés intéressants pour réduire la fraude, les pertes, les coûts de mise en œuvre, ainsi que d'autres coûts transactionnels. En substance, les *smart contracts* fonctionnent de manière comparable aux distributeurs de café ou de friandises : la machine livre le produit lorsque l'argent prévu a été inséré, sans latitude du côté du vendeur ni marge de négociation du côté de l'acheteur. Révolutionnaire à l'époque, l'idée de Nick Szabo paraît aujourd'hui élémentaire à la lumière de l'évolution des technologies. Depuis lors, les *smart contracts* « simples » se sont imposés.

Les *smart contracts* sont ainsi de plus en plus développés sur les blockchains de manière à tirer parti des avantages techniques et de la sécurité offerts par la technologie des registres distribués. Les systèmes décentralisés permettent d'éliminer les intermédiaires dans certaines transactions : gain de temps, et limitation des conflits liés à la négociation, à l'interprétation ou à l'exécution des contrats.

L'utilisation de blockchains pour y développer des « contrats intelligents » offre une sécurité accrue puisque les registres ne peuvent être altérés, modifiés ou détruits. La blockchain fait en sorte que les données, à commencer par le contenu des clauses convenues, sont sûres et immuables. Les parties ne peuvent modifier les termes de l'accord. Si une partie tente de modifier un contrat, une clause ou une transaction sur la blockchain, les protocoles du réseau distribué peuvent le détecter et l'empêcher. Cependant, l'impossibilité de modifier le code présente, dans le même temps, des difficultés. Les informations stockées sur la blockchain étant définitives, il n'est pas possible de modifier les modalités initiales d'un « contrat intelligent » sauf si une telle modification est prévue dans le code initial. Modifier un contrat (juridique) d'un commun accord est pourtant une pratique courante. Par conséquent, modifier des « contrats intelligents » qui n'ont pas été préprogrammés pour être modifiés se révèlera beaucoup plus difficile et coûteux que pour des contrats traditionnels, à supposer même qu'une modification soit possible.

D'autres avantages notables de l'utilisation de la blockchain pour développer des « contrats intelligents » tiennent au caractère automatique et à la vérifiabilité de leur exécution ainsi qu'à la diminution du niveau de confiance nécessaire. Le code du « contrat intelligent » s'exécutera de manière autonome sur le réseau chaque fois qu'un nœud le lira tout en vérifiant l'intégrité de la chaîne. Comme les parties n'ont pas de pouvoir discrétionnaire, une fois que les clauses sont convenues, écrites et inscrites dans la chaîne, les obligations sont exécutées sans aucune action de la part des parties au contrat. L'opération comporte parfois des modalités qui en renforcent la sécurité, tel le placement de fonds sur un compte séquestre virtuel (*escrow wallet*) avant une libération automatique des fonds lorsque l'opération est réalisée (si la marchandise est livrée par exemple). Les parties contractantes se voient ainsi offrir un moyen de faire respecter les obligations contractuelles et d'en assurer l'exécution sans avoir besoin de recourir à l'intervention de l'État (ou d'un tiers, quel qu'il soit).

Outre la réduction des coûts et la rapidité d'exécution, l'automatisation et l'absence de marge de manœuvre des parties présentent une série d'avantages majeurs en cas de manque de confiance dans une relation contractuelle et réduisent le besoin d'intermédiaires pour exécuter

ou faire respecter les obligations. Cependant, ces caractéristiques comportent également certains risques, car il est impossible d'empêcher l'exécution telle qu'elle a été conçue. Une transaction pourra être répétée en boucle. S'il y a une erreur, elle sera également répétée en boucle.

Enfin, les *smart contracts* comportent certaines limites techniques. Certaines sont liées à la technologie blockchain et d'autres sont inhérentes à la numérisation. Un contrat « intelligent » ne peut être aussi intelligent que son développeur et les ordinateurs qui l'exécutent. En outre, le programme ne peut pas faire plus que ce que permet l'état actuel de l'informatique, ce qui ne rend viables que certains types de *smart contracts* et d'usages. Comme le langage naturel ne peut être exécuté directement par un ordinateur, les contrats intelligents exigent que les obligations contractuelles soient traduites en termes informatiques lisibles et exécutables par ordinateur.

En outre, une limite importante des *smart contracts* tient à l'incapacité des blockchains à interagir avec les ressources et les données extérieures. Ce problème a été résolu grâce au développement de logiciels d'intermédiation appelés « oracles ». Les oracles relient les « contrats intelligents » à des ressources hors chaîne qui peuvent être des informations (telles la météo, l'heure d'arrivée d'un avion, l'arrivée d'un bien à destination), des signatures électroniques juridiquement contraignantes ou des paiements bancaires. En tant que tels, les oracles peuvent fournir des données déclenchant l'exécution d'un contrat intelligent, ou faire en sorte que les *smart contracts* déclenchent des actions hors chaîne comme par exemple ordonner à une institution financière de réaliser un paiement. Bien que les oracles offrent des possibilités infinies aux *smart contracts*, ils posent également des problèmes de sécurité spécifiques. En effet, alors que l'intérêt de la blockchain réside dans la suppression des tiers et du besoin de confiance dans une relation contractuelle, les oracles réintègrent ces aspects dans l'équation.

Cela étant, les oracles peuvent également contribuer à atténuer une autre limite importante des *smart contracts* en les connectant au monde physique. En effet, le développement de l'Internet des objets et des « biens intelligents » (*smart properties*) a permis aux *smart contracts* de se connecter à des objets utilisés dans la vie quotidienne comme les voitures, les serrures de porte, les luminaires, etc., élargissant ainsi le champ de l'automatisation. Pourtant, au-delà du monde numérique, il peut rester nécessaire de recourir aux méthodes traditionnelles d'exécution des obligations malgré leurs limites.

Il existe de nombreuses applications des « contrats intelligents ». Cependant, pour l'instant, ils sont principalement utilisés pour deux types de transactions : les transferts de fonds en crypto-monnaies lorsque certaines conditions sont remplies et l'imposition de pénalités financières lorsque certaines circonstances sont réunies. Ils peuvent apporter des gains d'efficacité dans l'exécution de contrats commerciaux de base, ou même faciliter les modes alternatifs de résolution des litiges. Dans le secteur de l'immobilier, ils peuvent faciliter les transactions grâce à des baux commerciaux intelligents, et éliminer les intermédiaires en permettant de placer des fonds sous séquestre, ce qui réduit les coûts. Dans le secteur des assurances, les « contrats intelligents » peuvent réduire les délais d'indemnisation des victimes assurées, en permettant par exemple de créditer automatiquement un voyageur assuré lorsqu'un oracle détecte un retard au départ ou à l'arrivée d'un avion. Dans le secteur de la logistique, les « contrats intelligents » peuvent garantir que les expéditeurs ne seront payés qu'après la livraison effective du colis au destinataire.

Le développement des « contrats intelligents » est toutefois limité par les problèmes de confidentialité découlant de la transparence de la technologie. Les *smart contracts* et les transactions étant enregistrés et visibles par tous, les utilisateurs étant potentiellement

réidentifiables, l'exécution de transactions sensibles ou confidentielles (par exemple le paiement des employés ou des fournisseurs) sur des blockchains publiques comme Ethereum paraît exclue tant que des solutions cryptographiques permettant de remédier à ce problème ne seront pas mises en œuvre.

En outre, plus le *smart contract* est complexe, plus son exécution est coûteuse. Par exemple, les *smart contracts* exécutés sur Ethereum nécessitent le paiement d'une redevance, appelée « gaz », pour que le programme soit exécuté sur la blockchain et que les transactions correspondantes soient ajoutées aux blocs. Plus les transactions du *smart contract* sont complexes, plus le prix du « gaz » est élevé. En raison de ce coût, les contrats intelligents restent pour l'instant relativement simples. Pourtant, de nouveaux protocoles et de nouvelles plateformes sont régulièrement développés pour alléger ces coûts et offrir plus de possibilités de développement des *smart contracts*.

Par conséquent, les *smart contracts* devraient, dans un avenir proche, permettre d'automatiser de nombreuses opérations, qu'il s'agisse de transférer des fonds, d'accroître le développement de l'Internet des objets ou de créer des places de marché entièrement automatisées. Les *smart contracts* d'aujourd'hui prévoient des paramètres et des modalités d'exécution relativement simples et précises. Mais les *smart contracts* devraient prochainement devenir de plus en plus complexes et permettre des transactions élaborées.

Références

G'sell, Florence (2019), Intelligence artificielle et blockchain, in Alexandra Bensamoun & Grégoire Loiseau, *Droit de l'intelligence artificielle*, Dalloz.

Martin-Bariteau, Florian & Marco Pontello (2020), *Hashing Out Agreements: An Overview of Smart Contracts under Canadian Law*.

Mik, Eliza (2017), Smart Contracts: Terminology, Technical Limitations and Real World Complexity, *Law, Innovation & Technology*.

Raskin, Max (2016), The Law and Legality of Smart Contracts, *Georgetown Law Technology Review* 1 : 2 306.

Surden, Harry (2012), Computable Contracts, *UC Davis Law Review* 46 : 629.

Szabo, Nick (1994), Smart Contracts – essais, publications et tutoriels par Nick Szabo.

Szabo, Nick (1996), Smart Contracts: Building Blocks for Digital Markets.

Szabo, Nick (1997), The Idea of Smart Contracts, publications et tutoriels par Nick Szabo.

Szabo, Nick (1997), Formalizing and Securing Relationships on Public Networks, *First Monday*.

Werbach, Kevin & Nicolas Cornell (2017), Contracts Ex Machina, *Duke Law Journal* 67 : 313.

Organisations autonomes décentralisées (DAO)

Une organisation autonome décentralisée (DAO, pour *Distributed Autonomous Organization*) est une organisation créée sur une blockchain pour permettre des actions et des prises de décisions collectives. De telles organisations informatisées s'appuient sur une multitude de *smart contracts* connectés entre eux pour faire fonctionner de manière autonome une organisation, sans leadership centralisé ni intervention humaine, sur un réseau pair-à-pair impliquant toutes les parties prenantes.

Les DAO peuvent avoir différents types d'architectures et d'objectifs. Toutes les règles habituelles en matière de gouvernance, d'adhésion et de fonctionnement sont codées dans les *smart contracts*. Si chaque *smart contract* est conçu pour accomplir des tâches spécifiques, ils peuvent collectivement accomplir des tâches relativement élaborées lorsqu'ils sont connectés ensemble et interagissent. Si les premières DAO fonctionnaient en impliquant une intervention

humaine, les dernières avancées permettent de créer des organisations décentralisées entièrement automatisées qui peuvent être des sociétés ou des coopératives à part entière. En intégrant des outils d'intelligence artificielle plus élaborés dans ces DAO, il sera possible à l'avenir de créer des organisations intelligentes, programmées pour agir de manière autonome et capables de s'adapter à l'évolution des circonstances.

En l'absence de gestion centralisée, l'organisation est entièrement gérée par un programme informatique. Les membres interagissent entre eux selon un protocole programmé dans le code : ils votent et donnent leur avis sur les décisions à prendre. À l'instar des actionnaires d'une société ou des membres d'une coopérative, les membres participent à la gouvernance des DAO en fonction des jetons de gouvernance qu'ils détiennent. Chaque jeton confère un droit de vote, mais aussi le droit de percevoir des dividendes, ou d'acquérir des avantages provenant de biens ou de services gérés par la DAO. Dans certains cas (mais pas toujours), plus un utilisateur possède de jetons de gouvernance, plus sa voix pèse dans les décisions.

Les DAO permettent une gouvernance plus sûre, plus transparente et plus responsable des organisations. La sécurité de la technologie blockchain garantit aux membres des DAO une plus grande certitude concernant la gestion de l'organisation et l'exercice des droits de vote, tout en permettant de réduire les abus potentiels. De même, comme tout est enregistré dans la blockchain, du code aux décisions prises, les parties prenantes sont davantage responsabilisées et les processus d'audit facilités. Si la DAO est gérée sur une blockchain publique, toute partie intéressée est en mesure de vérifier le fonctionnement de l'organisation. Cela peut être utile lorsque la confiance du public a été perdue ou est mise en cause. Toutefois, comme cela a été souligné précédemment pour les *smart contracts*, une telle transparence constitue aussi une limite et pourrait freiner l'adoption de la technologie par les entreprises.

La première DAO, appelée « The DAO », a été lancée en 2016 sur la plateforme Ethereum pour faciliter le financement participatif de divers projets. Les investisseurs apportaient des crypto-monnaies et recevaient en échange des jetons leur accordant des droits de vote sur les propositions de financement présentées à la DAO. Les investisseurs ayant financé la DAO disposaient d'un droit sur les bénéfices réalisés par les projets financés par la DAO, au prorata des jetons détenus. Depuis, de nombreuses autres DAO ont vu le jour. Par exemple, la MolochDAO a pour objet de permettre à ses membres d'apporter des capitaux à Ethereum au motif que cette blockchain constitue un bien public et une infrastructure essentielle. La coopérative d'investissement finlandaise Robin Hood Coop utilise une DAO pour gérer les actifs des membres de la coopérative. En Allemagne, Koina utilise une blockchain privée pour fournir un système monétaire permettant aux producteurs d'obtenir des crédits pour financer de manière indépendante leurs activités futures. Plus récemment, la ConstitutionDAO s'est formée dans un seul but : lever des fonds pour acheter un jeton non fongible (NFT) de la Constitution des États-Unis d'Amérique ; mais elle a perdu les enchères.

Références

Buterin, Vitalik (2014), DAOs, DACs, Das and More: An Incomplete Terminology Guide.

G'sell, Florence (2019), Intelligence artificielle et blockchain, in Bensamoun, Alexandra & Loiseau, Grégoire (2019), *Droit de l'intelligence artificielle*, Dalloz.

Metjahic, Laila (2018), Deconstructing the DAO: The need for legal recognition and the application of securities laws to decentralized organizations, *Cardozo Law Review* 39 : 1533.

Szabo, Nick (1994), Smart Contracts.

Wright, Aaron & Primavera De Filippi (2015), Decentralized Blockchain Technology and the Rise of Lex Cryptographia.

Jetons non fongibles (NFT)

Un jeton non fongible (NFT, pour *Non-Fungible Token*) est une unité de données non fongible stockée sur une blockchain qui peut être transférée entre utilisateurs. Contrairement aux crypto-monnaies telles que le Bitcoin, qui sont composées de jetons fongibles où chaque unité de Bitcoin est interchangeable avec toute autre unité de bitcoin, les NFT ne sont pas mutuellement interchangeables. S'appuyant sur l'idée des « biens intelligents » (« *smart properties* ») de Nick Szabo, les NFT permettent la marchandisation et l'échange d'actifs numériques tangibles ou intangibles, qu'il s'agisse du GIF d'un chat volant, d'une maison, de billets de concert ou de loterie, ou encore de prêts.

Les NFT ont gagné en popularité en 2021, notamment dans le monde de l'art, afin de soutenir les artistes numériques. Cette technologie a fait les gros titres lorsque la maison de vente aux enchères Christie's a facilité la vente inédite d'un NFT de l'artiste numérique Beeple pour 69 millions de dollars américains. La plupart des œuvres d'art numérique qui sont des NFT dépeignent de manière nostalgique les 8 bits des débuts de l'ère Internet. Mais à mesure que cette technologie devient plus accessible, les artistes abordent des sujets de société plus sensibles. Par exemple, l'artiste chinois dissident Badiucao a publié une collection de NFT sur le thème des Jeux olympiques, critiquant le bilan de la Chine en matière de droits de l'homme. La plateforme NFT qu'il a mise en place permet aux citoyens de contribuer à la collection en y ajoutant leurs propres œuvres.

Les NFT permettent de créer des biens numériques rares et de gérer les différents droits, des droits d'auteur à la propriété de l'œuvre elle-même. Ils s'appuient sur le registre de la blockchain pour fournir des certificats sécurisés d'authenticité ou de propriété. En outre, des *smart contracts* facilitent les ventes et paiements directs entre les parties et offrent la possibilité de verser automatiquement des redevances de droits d'auteur aux artistes. Cette compensation financière provenant de la vente sur le marché secondaire des biens représentés par le jeton est un élément attrayant tant pour les artistes numériques que pour les spéculateurs — ce qui explique, en partie, le succès des NFT.

Il existe différents types de NFT, mais le plus courant est un fichier de métadonnées contenant des informations codées avec une version numérique du bien sous forme de token (titre, œuvre d'art, etc.). Une autre possibilité consiste à télécharger l'œuvre entière sur la blockchain. Cette option a un coût important et est, par conséquent, moins populaire. La plupart des NFT sont développés selon la norme ERC-721 sur la blockchain Ethereum. À la base, un NFT comprend deux éléments : l'identité du jeton (un numéro généré lors de la création du jeton), et l'adresse du contrat qui renvoie à l'emplacement du contrat intelligent gérant la propriété et la logique du NFT. Cette combinaison rend le NFT unique, ce qui signifie qu'il n'existe qu'un seul jeton au monde avec cette combinaison d'identité de jeton et d'adresse de contrat. En outre, le NFT peut inclure l'adresse du portefeuille numérique de son créateur, ce qui, à condition d'utiliser la norme EIP-2981, permet audit créateur d'exiger et d'automatiser le paiement de redevances et de droits sur les ventes ultérieures du NFT.

Les NFT comprennent souvent un lien vers l'œuvre originale symbolisée par le jeton. Le NFT n'est pas, en fait, l'œuvre elle-même, mais plutôt une représentation numérique unique liée d'une manière ou d'une autre à l'œuvre originale. En particulier, si les NFT peuvent représenter numériquement des droits sur un bien matériel ou immatériel, ils ne confèrent pas nécessairement des droits de propriété sur ce bien. Par exemple, la vente d'une œuvre d'art représentée par un NFT peut transférer la propriété du jeton, mais ne transfère pas nécessairement les droits d'auteur attachés à l'œuvre. De même, la capacité d'enregistrement

de la blockchain ne protège pas contre les copies et les infractions en dehors de la blockchain hébergeant le NFT.

Récemment, un groupe connu sous le nom de SpiceDAO a acheté le NFT correspondant à l'interprétation cinématographique prévue du roman *Dune* du cinéaste Alejandro Jodorowsky. Mais SpiceDAO ignorait que ce jeton de 3 millions de dollars ne comprenait ni les droits d'auteur, ni les droits de reproduction du livre.

Références

Angeleti, Gabriella (2022), Crypto group shamed for spending $3m on 'Dune' book, mistakenly believing it had acquired copyright to produce NFTs.

Burks, Zach, James Morgan, Blaine Malone & James Seibel (2020), EIP-2981: NFT Royalty Standard.

Christie's Auction House (2021), Beeple's opus.

Cooper, James & Peter Grazul (2021), NFTs for freedom: Nonfungible tokens and the right to self-determination.

Entriken, William, Shirley Dieter, Jacob Evans & Nastassia Sachs (2018), EIP-721: Non-Fungible Token Standard.

Griffith, Erin (2021), Why an Animated Flying Cat with a Pop-Tart Body Sold for Almost $600,000.

Guadamuz, Andres (2021), Non-fungible tokens (NFTs) and copyright.

Harris, Gareth (2022), Badiucao launches NFT collection to protest against China's human rights record on even of Beijing Winter Olympics.

Mediapedia (2018), The Various types of Crypto Tokens.

Reyburn, Scott (2021), JPG File Sells for $69 Million, as 'NFT Mania' Gathers Pace.

Critiques suscitées par les blockchains

La technologie blockchain et son écosystème font l'objet d'un important battage médiatique et d'un véritable engouement. Néanmoins, il convient de réfréner cet enthousiasme. Il s'agit certainement d'une technologie puissante aux nombreuses applications, souvent présentée par ses défenseurs comme une panacée. Cependant, comme nous l'avons souligné, cette présentation est assez éloignée de la réalité. Cette technologie n'est pas la solution à tous les problèmes ni adaptée à tous les besoins. Les caractéristiques de transparence et d'immutabilité peuvent être contre-productives et entraîner, dans certains cas, de nouveaux risques. De plus, malgré les idées reçues, la sécurité de la blockchain n'est pas à toute épreuve. Elle est subordonnée à l'absence de coalition des nœuds du réseau et au fait que les utilisateurs conservent de manière sécurisée leurs informations d'identification. En outre, des erreurs dans le code ou le protocole de gouvernance de la blockchain peuvent permettre à des acteurs malveillants de prendre le contrôle de certains actifs ou transactions. L'année passée, ces scénarios supposés théoriques se sont réalisés.

Par ailleurs, bien que très en vogue, la technologie blockchain a été vivement critiquée pour son impact sur la société. Les crypto-monnaies — comme le Bitcoin — ont souvent été associées à des activités criminelles. Certes, dans un premier temps, les délinquants ont exploité ces outils et développé de nouvelles arnaques en se servant de l'engouement financier pour les crypto-actifs. Des acteurs malveillants et des groupes haineux ont utilisé les crypto-actifs pour se financer. Toutefois, ces comportements ne sont pas nouveaux ou propres à l'écosystème blockchain. En outre, les services de police et les tribunaux ont désormais compris la technologie – et les modalités de la lutte contre le blanchiment d'argent ont été mises à jour en

conséquence. D'importantes plateformes illicites, comme la tristement célèbre Silk Road, ont été démantelées et de nouvelles réglementations permettent de réprimer les activités criminelles.

L'utilisation des blockchains suscite également des préoccupations et des critiques en matière environnementale. La création de crypto-actifs, de « contrats intelligents », de DAO et de NFT fait l'objet d'une controverse en raison de la forte consommation d'énergie associée aux transactions sur les blockchains, et des émissions de gaz à effet de serre qui en découlent. En effet, les blockchains — notamment celles qui reposent sur le protocole de la « preuve de travail » — nécessitent une importante puissance de calcul, et donc de l'énergie générant d'importantes émissions de carbone. En juin 2018, la Bank for International Settlements a critiqué l'utilisation du « proof of work » en raison de la forte consommation d'énergie qu'il entraîne.

Une récente étude de l'Université de Cambridge a conclu qu'en 2022, les blockchains Bitcoin et Ethereum émettront ensemble près de 120 millions de tonnes de CO_2 par an. En novembre 2021, l'Autorité de surveillance financière et l'Autorité de protection de l'environnement suédoises ont appelé à une interdiction du minage de crypto-monnaies à forte consommation énergétique, affirmant que les crypto-actifs constituent une menace pour la transition climatique. Les deux autorités ont examiné les avantages potentiels de la blockchain et ont estimé qu'ils étaient contrebalancés par la consommation d'énergie et l'empreinte carbone « énormes ». Elles estiment que sans une interdiction à l'échelle européenne des techniques de minage les plus énergivores, l'UE ne sera pas en mesure d'atteindre ses objectifs climatiques. Bien que contestée, l'interdiction de la « preuve de travail » a également été défendue par le vice-président de l'Autorité européenne des marchés financiers. Il convient de noter que l'impact environnemental du minage pourrait être jugé contraire au droit à un environnement sain, tel que protégé par la Cour européenne des droits de l'homme en vertu de son interprétation constructive des articles 2, 5 et 8 de la Convention européenne des droits de l'homme.

Face à ces critiques, les développeurs se tournent vers des protocoles de minage moins énergivores comme le « preuve de participation » (« *proof of stake* »). En effet, la plateforme Ethereum passera à un tel protocole en 2023. D'autres options consistent à envisager de déplacer certaines opérations hors chaîne pour ne conserver que les éléments clés qui doivent être automatisés ou qui risquent d'être falsifiés.

En outre, les mineurs de crypto-actifs sont désireux d'utiliser davantage d'énergie renouvelable, et certaines initiatives visent à recycler la chaleur générée par les activités de minage. En Colombie-Britannique, MintGreen s'est associé à la ville de North Vancouver pour réutiliser la chaleur produite afin de chauffer une centaine de maisons et de bâtiments industriels. En France, WiseMining a développé des chaudières de minage grâce auxquelles les utilisateurs peuvent chauffer leur maison en minant des bitcoins. Les mineurs de crypto-actifs renforcent également leur présence dans les régions à climat froid dans lesquelles les ordinateurs refroidissent naturellement ce qui permet de réduire les factures et la consommation d'énergie. Ils s'installent également dans les pays où l'énergie est peu chère ou subventionnée. Pourtant, les considérations d'ordre énergétique peuvent comporter des risques de gouvernance et de géopolitique pour les plateformes blockchain. En effet, elles pourraient conduire à une concentration de groupes de mineurs dans des régions particulières, ce qui pourrait menacer la gouvernance du réseau distribué. Si 51% des mineurs d'une blockchain se trouvent dans le même pays, le réseau risque d'être contrôlé ou perturbé par le gouvernement dudit pays.

Références

Association pour le développement des actifs numériques (2022), Interdiction du proof-of-work en Europe : une réponse inappropriée à des questions compréhensibles.

Cambridge Centre for Alternative Finance (2022), Comparisons, Cambridge Bitcoin Electricity Consumption Index.

de Vries, Alex, Ulrich Gallersdörfer, Lena Klaaßen & Christian Stoll (2002), Revisiting Bitcoin's carbon footprint, Joule.

Shin, Hyun Song (2018), Chapter V. Cryptocurrencies: looking beyond the hype, *BIS Annual Economic Report*, Banque des règlements internationaux.

The Economist (2022), The charm of cryptocurrencies for white supremacists.

Thedéen, Erik & Björn Risinger (2021), Crypto-assets are a threat to the climate transition—energy-intensive mining should be banned, Finansinspektionen – Autorité suédoise de surveillance financière.

Weinstein, Jason (2021), Why Bitcoin is Better for Crime Fighters than Criminals.

2. Opportunités pour les droits de l'homme et la démocratie

La technologie blockchain offre aux pouvoirs publics, aux organisations internationales, aux ONG, aux entreprises et au grand public les moyens d'œuvrer à la reconnaissance et au respect des droits de l'homme et à la résolution de difficultés qui se posent dans ce domaine.

Avant tout, la technologie blockchain peut permettre de renforcer l'exercice des libertés fondamentales en facilitant le pseudo-anonymat des utilisateurs sur Internet. Dans le même temps, les blockchains constituent des plateformes permettant de développer des identités numériques sécurisées, et notamment des identités auto-souveraines susceptibles de servir de documents d'identité aux réfugiés et aux migrants. La technologie pourrait également permettre l'autonomie personnelle en redonnant aux citoyens le contrôle sur leurs données.

Compte tenu de ces capacités, les fonctionnalités de la blockchain ont été exploitées dans le contexte humanitaire pour renforcer la transparence des procédures, soutenir la distribution de l'aide humanitaire, fournir des services financiers aux personnes sans compte bancaire et garantir des salaires décents aux travailleurs. Les blockchains peuvent également aider à lutter contre les violations des droits de l'homme dans le cadre des chaînes d'approvisionnement et à sécuriser les propriétés immobilières. Il a aussi été proposé de recourir à la technologie blockchain pour soutenir le fonctionnement des institutions démocratiques, par exemple pour mettre en place des plateformes de vote sécurisées et permettre d'élaborer des lois de manière collaborative. En outre, les blockchains et les *smart contracts* ont été utilisés pour mettre en place de nouveaux mécanismes de résolution des conflits. Ils ont également indiqués pour faciliter le travail des tribunaux étatiques et permettre une meilleure conservation des preuves.

Ce ne sont là que quelques exemples de la manière dont la technologie peut être utilisée pour faire progresser le fonctionnement de la démocratie et garantir la transparence et la prise de responsabilité. La présente section décrit certaines des applications actuelles et potentielles de la technologie blockchain permettant de renforcer la protection des droits de l'homme et le fonctionnement de la démocratie, ainsi que donner davantage de pouvoir aux citoyens, voire même aux populations défavorisées. La technologie blockchain est un plein développement – son utilité pour la protection et le respect de droits de l'homme est donc promise à se renforcer. Au cours des prochaines années, il importera que les acteurs du secteur technologique, les États et les citoyens se familiarisent avec la technologie blockchain qui apparaîtra de plus en plus comme une ressource inestimable permettant d'améliorer le respect des valeurs démocratiques dans le monde entier.

Améliorer l'exercice des libertés grâce au pseudo-anonymat

Sur les blockchains publiques, le pseudo-anonymat des utilisateurs prévaut. Comme décrit plus haut, seule leur adresse publique est visible et il est, en principe, impossible de savoir qui se cache derrière une adresse publique. Une telle adresse peut cacher une entreprise, une institution ou une personne physique.

Certes, le pseudo-anonymat qui prévaut sur les blockchains comporte des risques souvent dénoncés. Les transactions en crypto-monnaies pourraient faciliter la fraude fiscale, permettre le blanchiment massif d'argent sale et financer le terrorisme. Cependant, ce pseudo-anonymat offre concomitamment des garanties en termes de libertés et de vie privée. En effet, même si

toutes les transactions sont, en principe, transparentes sur les blockchains ouvertes, ces transactions ne sont pas explicitement liées à des individus ou des organisations existant dans le monde physique. Il est ainsi possible de protéger l'identité des parties, de leur garantir une pleine liberté d'action et de protéger leurs données personnelles.

Avantages du pseudo-anonymat pour les libertés fondamentales

Le pseudo-anonymat inhérent à la technologie blockchain garantit le respect des libertés. Par exemple, le fait d'être anonyme en ligne peut conditionner la liberté d'expression des personnes. Il est indiscutable que l'anonymat protège la liberté des individus de communiquer des informations et des idées qu'ils seraient autrement empêchés d'exprimer. De même, l'anonymat garantit la liberté des individus de vivre leur vie privée. Ces considérations expliquent pourquoi le « droit à l'anonymat » est pour beaucoup une garantie essentielle, à tel point que l'organisation ARTICLE 19 considère l'anonymat comme un droit fondamental, qui inclut le droit de s'exprimer, de lire et de naviguer en ligne de manière anonyme. Dans cette perspective, le chiffrement est considéré comme une exigence fondamentale pour la protection de la confidentialité des informations et leur sécurité, qui est essentielle à la protection du droit à la liberté d'expression en ligne. Garantir un pseudo-anonymat effectif sur les plateformes blockchain est non seulement nécessaire pour préserver la vie privée en général, mais aussi pour assurer la protection des données personnelles dès lors que la protection des données n'est plus garantie si les personnes concernées sont identifiables. À cet égard, le pseudo-anonymat que permet la technologie blockchain va dans le sens des objectifs du *Règlement général sur la protection des données* de l'Union européenne et ceux de la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* (Convention 108).

Limites du pseudo-anonymat

La portée du pseudo-anonymat garanti par la blockchain doit cependant être nuancée. En effet, comme expliqué précédemment, il est souvent possible de découvrir l'identité réelle des utilisateurs. Sur les blockchains privées et à permissions dont l'accès est limité à un petit nombre de personnes, l'identité des utilisateurs est *a priori* connue de celui qui administre la plateforme. Sur les blockchains publiques et ouvertes, les utilisateurs sont souvent contraints de révéler leur identité. En effet, pour stocker et transférer des crypto-actifs, les utilisateurs créent généralement un portefeuille en ligne auprès d'un prestataire de services, ce qui implique habituellement de révéler son identité. La réglementation en matière de lutte contre le blanchiment d'argent impose aux prestataires des obligations similaires à celles imposées aux services financiers traditionnels, telles que l'identification de leurs clients dans le cadre de l'obligation de « connaissance du client » (KYC), la surveillance des activités des clients et la déclaration aux autorités nationales de renseignement financier. Les plateformes effectuent donc des contrôles et exigent des preuves d'identité, telles qu'une copie d'un permis de conduire, un passeport ou une facture. En pratique, de nombreux portefeuilles numériques sur ces plateformes sont liés à des comptes bancaires réels ou à des cartes de crédit ou de débit.

Certes, il est toujours possible pour les utilisateurs de ne pas créer de portefeuille en ligne et de stocker leur clé privée hors ligne de manière complètement déconnectée d'Internet (sur un disque dur externe ou sur papier) ce qui permet d'éviter de divulguer son identité. Il est également possible de stocker sa clé privée directement sur son ordinateur. Mais, même dans ces dernières hypothèses, les risques de ré-identification sont réels : dans la mesure où il est possible, sur une blockchain publique, de tracer toutes les transactions provenant d'une adresse publique donnée, la ré-identification du propriétaire de l'adresse à partir d'éléments connus est possible à l'aide d'outils d'apprentissage automatique.

Renforcer l'anonymat sur les blockchains

Un certain nombre de techniques ont été développées pour renforcer l'anonymat sur les blockchains. De nouvelles crypto-monnaies appelées « *privacy coins* » ont vu le jour dans le but de garantir un véritable anonymat et de protéger la vie privée. Des crypto-monnaies récentes, comme Monero, Zcash et Dash, ont été spécifiquement conçues pour garantir l'anonymat de leurs utilisateurs. Ces crypto-monnaies utilisent des technologies renforçant l'anonymat pour empêcher la révélation des détails des transactions ou pour rendre très difficile le suivi des transactions. Il s'agit notamment des techniques de « preuve à divulgation nulle de connaissance » ("*Zero-Knowledge Proof*", ZKP), des adresses furtives ou des signatures circulaires.

Les techniques de « preuve à divulgation nulle de connaissance » (ZKP) constituent l'une des évolutions les plus prometteuses en matière de protection de la vie privée. Il s'agit de répondre à une question binaire (vrai/faux) sans jamais avoir à révéler les informations étayant l'affirmation. Cela permet, par exemple, à une personne qui affirme avoir plus de 18 ans de l'attester sans divulguer sa date de naissance. Il lui suffit de scanner un code QR et de demander à un algorithme d'effectuer une opération qui renvoie simplement une réponse « oui » ou « non » à la question de savoir si la personne est majeure. À aucun moment, la personne n'a besoin de révéler d'autres informations, ce qui préserve sa vie privée. Cette technique peut également être utilisée pour prouver d'autres faits, comme le fait qu'une personne est autorisée à travailler dans un pays sans avoir à divulguer son état civil ou sa nationalité. Il est également possible, grâce à cette technique, de publier des transactions sur la plateforme Zcash sans donner de détails, par exemple, sur leur montant ou les adresses publiques concernées. En outre, les protocoles ZKP permettent de supprimer les liens historiques entre les transactions. Les utilisateurs prouvent qu'ils possèdent les jetons au moment de l'échange, puis les jetons sont détruits pour faire place à de nouveaux jetons vierges (sans historique) qui seront utilisés dans la transaction. Comme il n'existe aucune relation entre les nouveaux jetons et les jetons détruits, il est impossible d'établir un lien entre un jeton et un utilisateur.

D'autres techniques sont utilisées pour éviter la ré-identification. Par exemple, une nouvelle paire de clés (publique/privée) peut être utilisée pour chaque transaction. Les transactions peuvent également être regroupées de manière à ce qu'il soit impossible de discerner les parties à la transaction, ou à ce que leur identité soit cachée dans d'autres transactions en liant une seule transaction à plusieurs clés publiques, même si la transaction provient d'une seule des clés publiques. Parfois, les techniques sont combinées pour une plus grande efficacité. Ainsi, sur la plateforme Monero, il est possible de cacher le montant de la transaction et l'adresse publique de l'expéditeur et du destinataire par une combinaison de techniques, notamment le fait que pour chaque transaction, une nouvelle adresse publique et une clé privée correspondante sont générées.

Parallèlement aux « *privacy coins* », certaines initiatives visent simplement à créer des environnements respectueux de la vie privée, comme Oasis Network et Secret Network, conçus pour exécuter des contrats intelligents dans un environnement de confidentialité par défaut afin de protéger les données des utilisateurs ainsi que la confidentialité des transactions. Par exemple, les nœuds de Secret Network traitent et stockent les données dans des environnements sécurisés qui fonctionnent comme une « boîte noire » ne pouvant être manipulée. Les données étant chiffrées et confidentielles par défaut, les utilisateurs disposent de « clés de visualisation » pour consulter leurs données sensibles. Elles permettent aux utilisateurs de garder le contrôle de leurs données et de décider ce qui est partagé et avec qui.

Les progrès des techniques d'anonymisation peuvent à juste titre inquiéter les autorités qui craignent la prolifération d'activités frauduleuses et illégales. Il est donc important de trouver

un juste équilibre entre l'impératif de protection de la vie privée et des données, et l'objectif de lutte contre les activités illégales. Il ne faut pas non plus oublier que la prévention des comportements répréhensibles prime souvent sur les exigences de protection des données, même dans le cadre du RGPD (considérant 19).

Références

ARTICLE 19 (2015), Right to Online Anonymity: Policy Brief.

ARTICLE 19 (2019), Blockchain and freedom of expression.

Ferdous, Md Sadek, Farida Chowdhury, & Madini Alassafi (2019), In Search of Self-Sovereign Identity, Leveraging Blockchain Technology, IEEE.

Fink, Michèle (2019), Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?, European Parliamentary Research Service.

Zyskind, Guy, Oz Nathan & Alex « Sandy » Pentland (2015), Enigma: Decentralized Computation Platform with Guaranteed Privacy.

Zyskind, Guy (2021), Introducing SCRT Labs—An Evolution of Enigma.

Gérer des identités numériques

Traditionnellement, l'autorité habilitée à établir l'identité des personnes est l'État, qui le fait sur la base de ses propres méthodes d'identification. L'État établit l'identité officielle des personnes à partir de différentes informations (nom, sexe, date de naissance, lieu de résidence, etc.) et délivre des documents d'identité officiels sur cette base. Les choses sont différentes dans le monde virtuel. La question de l'identification des personnes en ligne s'est posée avec les premiers réseaux informatiques. Dès l'origine, les outils utilisés par les internautes comportaient des moyens permettant d'identifier plus ou moins les utilisateurs en utilisant, par exemple, l'adresse IP. Cependant, avec l'augmentation du nombre d'échanges et de transactions en ligne, des méthodes d'identification plus poussées sont devenues nécessaires et ont été progressivement proposées par les fournisseurs de services numériques. Ces fournisseurs ont développé des systèmes centralisés de gestion d'identité numérique. Sur la base de certaines informations fournies par les utilisateurs, ces systèmes leur attribuent un « identifiant », qui peut correspondre, selon le cas, à l'identité officielle de l'utilisateur ou à un pseudonyme et peut être lié à un certain nombre d'informations. Par exemple, pour effectuer des achats en ligne, l'utilisateur doit s'inscrire sur un site de commerce électronique et fournir ses nom, adresse, e-mail, téléphone, coordonnées bancaires, etc.

Dans le monde virtuel, il existe ainsi des « tiers de confiance » qui ont le pouvoir de définir les méthodes d'identification d'une personne, d'attribuer un « identifiant » à cette personne et de sécuriser leur identification à l'aide de justificatifs (par exemple, mots de passe, code, informations diverses). Ces « tiers de confiance » sont des entités privées. Certains délèguent l'authentification à ces tiers de confiance : tel est le cas, par exemple, lorsque les utilisateurs sont invités à se connecter avec leur adresse électronique ou avec l'identifiant d'un réseau social. Souvent, ces services d'identification sont proposés par de grandes entreprises technologiques (comme Apple, Google, Facebook) qui sont en mesure de fournir des services d'identification fiables et sécurisés. En 2008, la création de Facebook Connect a permis à Facebook (désormais Meta) d'occuper une place de plus en plus importante sur le marché de l'identité numérique.

Cependant, le recours à ces « tiers de confiance » est très problématique, car il rend les utilisateurs dépendants de grandes plateformes qui contrôlent les comptes et ont toujours la possibilité de couper arbitrairement leur accès aux services en ligne. En outre, les utilisateurs sont tenus de partager une grande quantité d'informations personnelles, sans toujours savoir quel usage sera fait de leurs données. En effet, les plateformes profitent de leur activité de gestion d'identité pour collecter systématiquement les données des utilisateurs, les suivre et pratiquer la publicité ciblée. Dans un tel environnement, les données des individus sont détenues par un certain nombre d'entités privées, qui possèdent des informations que les utilisateurs ont été contraints de partager avec elles pour pouvoir réaliser des transactions en ligne. Enfin, la sécurité de ces données n'est pas toujours garantie, car les fuites de données et les usurpations d'identité restent fréquentes dans le monde virtuel.

Dans un tel contexte, la technologie blockchain pourrait permettre aux utilisateurs d'échapper au contrôle des grandes entreprises technologiques. Les structures décentralisées permettent le développement de nouveaux modèles de gestion des identités numériques dans lesquels les utilisateurs conservent le contrôle sur leur identité : on parle d'« identité autonome » (SSI, pour *Self-Sovereign Identity*). On dit parfois que la SSI pourrait même concurrencer le monopole actuel des identités attribuées par l'État. Si cette position peut sembler exagérée, un système de SSI peut toutefois compenser l'absence de documents d'identité délivrés par l'État, soit parce qu'ils ont été perdus ou détruits, soit, tout simplement, parce que l'État en question ne les a pas fournis. Il pourrait également être utile dans les cas où le document d'identité n'est pas reconnu par un État, par exemple en cas de conflits diplomatiques.

Le contrôle de l'identification : la notion d'« identité autonome » (SSI)

Le développement de l'« identité autonome » ou « identité auto-souveraine » (SSI, pour *Self-Sovereign Identity*) vise à placer les utilisateurs au centre de leur identité numérique en leur permettant de contrôler leur propre identité virtuelle. Depuis le début des années 2000, les nouvelles méthodes de création d'identités numériques sont centrées sur le consentement de l'utilisateur et l'objectif d'interopérabilité. Le but est que les utilisateurs n'aient plus besoin de divulguer des informations personnelles à chaque fois qu'ils se connectent à des sites Internet. Or il n'est pas possible de laisser véritablement le contrôle aux utilisateurs dans le cadre de réseaux centralisés où des entreprises privées gèrent les identités. Seules les technologies décentralisées peuvent donner aux utilisateurs le pouvoir de contrôler leur identité numérique. C'est ainsi que le concept d'identité décentralisée est apparu pour permettre aux utilisateurs de gérer leur propre identité et de contrôler les informations qu'ils partagent sous forme de certificats. En termes simples, une identité décentralisée permet le contrôle total, personnel et entier de toutes les informations relatives à l'utilisateur. Les identités décentralisées ne sont pas déterminées et détenues par chaque plateforme, mais font partie d'un réseau décentralisé conçu de telle sorte que les utilisateurs conservent le contrôle de leur identité tout en étant capables de s'authentifier partout avec la même identité. La décentralisation soutient également l'objectif de minimisation des données en ne fournissant que les informations nécessaires à la plateforme visitée. Si un âge minimum est requis, le système peut confirmer que le seuil est atteint sans divulguer l'âge exact ; si l'âge est requis, le système peut le confirmer sans divulguer la date de naissance exacte.

La technologie blockchain permet le développement d'un tel système d'identité décentralisé dans lequel les identifiants et les informations sont détenus et contrôlés par les utilisateurs plutôt que par des organisations centralisées. En effet, les utilisateurs sont déjà identifiés, sur la blockchain, par une clé publique visible par tous et une clé privée qui leur est personnelle et garantit leur contrôle. Seule la personne qui détient la clé privée a accès au compte et aux

éléments qui y sont associés. L'idée est de tirer parti de cette infrastructure technique pour identifier et authentifier sans erreur possible une personne ou une organisation sans avoir à s'appuyer sur une autorité gouvernementale ou un registre centralisé.

La création d'une telle identité autonome ou décentralisée (SSI) basée sur la blockchain implique de disposer d'une application de portefeuille numérique qui permet la création d'identifiants numériques SSI. Lorsque le portefeuille est créé, un ou plusieurs identifiants décentralisés (DID pour *Decentralized Identifier*) sont générés et attribués. Un identifiant décentralisé est une URL associée à une identité unique, qui peut se présenter sous la forme d'un code QR. Le DID relie l'individu à un Document DID qui contient toutes les informations publiques sur la personne identifiée, à commencer par une clé publique désignant celui qui contrôle le document. Le Document DID est public, accessible à tous, et ne peut être modifié que par son contrôleur officiel grâce à la clé privée de celui-ci.

Alors que le Document DID contient des informations publiques, les informations à partager sont stockées sous forme de « justificatifs vérifiables » (VC pour *Verifiable Credentials*). Une fois le portefeuille d'identité numérique créé, il est possible pour son détenteur de collecter des justificatifs auprès de diverses organisations autorisées à délivrer numériquement de tels justificatifs. Ces VC établis et signés par des tiers de confiance, attestent de la véracité de certaines informations. Ils peuvent être délivrés par diverses entités telles que les États (par exemple, des justificatifs d'identité), les universités (par exemple, des diplômes) ou des compagnies d'assurance (par exemple, l'attestation d'une couverture santé). Chaque VC est signé numériquement par la clé privée de l'organisme émetteur, ce qui permet de vérifier la fiabilité du justificatif en consultant l'émetteur du Document DID. Le portefeuille numérique peut également inclure des liens vers des données stockées dans le cloud, tels des dossiers médicaux cryptés. Le détenteur de l'identité décentralisée peut, si nécessaire, décider de donner l'autorisation d'accéder à ces informations à ceux qui souhaitent les consulter.

Les systèmes d'identités décentralisées présentent de nombreux avantages. Ils permettent aux utilisateurs de créer plusieurs identités numériques, de naviguer discrètement en ligne en présentant leurs justificatifs sans être tracés, et de limiter le volume des données collectées sur les utilisateurs. Ils offrent également les garanties de sécurité offertes par la décentralisation, puisque les données ne sont pas stockées par une seule autorité centralisée. Ils réduisent considérablement le risque d'usurpation d'identité et, plus largement, de fraude. Enfin, ils permettent de gérer toutes sortes d'informations officielles : certificats de naissance ou de mariage, passeports, visas, permis de séjour, diplômes, documents de sécurité sociale, etc.

Des solutions sont actuellement développées sur des blockchains publiques et sans permissions comme uPort (maintenant Veramo), Jolocom ou Sovrin. Certaines solutions sont développées sur des blockchains de consortium comme KYC Chain ou ID2020. Le projet Civic a proposé un système de vérification d'identité unifié pour l'écosystème décentralisé où les utilisateurs du Civic Pass peuvent télécharger une application et la configurer avec diverses informations d'identité personnelles (nom, adresse, numéro de sécurité sociale, numéro de passeport, permis de conduire, etc.) L'application chiffre ces données à l'aide d'une clé privée émise par un tiers, ce qui garantit que Civic n'accède pas aux informations d'identité personnelle sans le consentement des utilisateurs. La biométrie multifactorielle (par exemple, la numérisation des empreintes digitales) sécurise l'application et permet aux utilisateurs de garder le contrôle de leurs données. L'application ne stocke que les informations d'identification, et non les données de l'utilisateur lui-même. Les utilisateurs peuvent ensuite utiliser leur Civic Pass pour être authentifiés sur diverses plateformes sans fournir leurs informations personnelles à ces plateformes.

Cependant, il est peu probable que les systèmes d'identités décentralisées permettent de se passer entièrement du rôle des États dans l'attestation de l'identité des personnes. En effet, les systèmes SSI exigent que les justificatifs soient délivrés par des émetteurs de confiance, et les autorités gouvernementales seront toujours nécessaires pour fournir des informations fiables. Toutefois, l'utilisation de solutions d'identité numérique basées sur la blockchain peut aider tous ceux qui ne disposent pas de documents officiels, soit parce qu'ils n'en ont jamais eu, soit parce qu'on leur a fourni de faux documents (comme c'est souvent le cas pour les migrants), soit parce que ces documents officiels ont été détruits ou perdus.

Références

Allen, Christopher (2016), The path to self-sovereign identity.

Bajpai, Prableen (2017), How Blockchain Can Help Humanitarian Causes.

Crumpler, William (2021), The Human Rights Risks and Opportunities in Blockchain, CSIS.

Desai, Vyjayanti, Anna Diofasi & Jing Lu, (2018), The global identification challenge: Who are the 1 billion people without proof of identity?, World Bank Blogs.

Der, Uwe, Stefan Jähnichen & Jan Sürmeli (2017), Self-sovereign Identity—Opportunities and Challenges for the Digital Revolution.

Ferdous, Md Sadek, Farida Chowdhury, & Madini Alassafi (2019), In Search of Self-Sovereign Identity, Leveraging Blockchain Technology, IEEE.

Lyons, Tom, Ludovic Courcelas & Ken Timsit (2019), Blockchain and digital identity, Observatoire-forum des chaînes de blocs de l'Union européenne.

W3C (2021), Decentralized Identifies (DIDs), v1.0: Core architecture, data model and representation.

Wang, Fennie & Primavera De Filippi (2020), Self-Sovereign Identity in a Globalized World: Credentials-Based Identify Systems as a Driver for Economic Inclusion, *Frontiers in blockchain 2*.

Permettre l'autodétermination informationnelle

Les blockchains peuvent offrir des solutions alternatives de gestion des données, car elles permettent de partager les données de manière transparente et décentralisée. Cette capacité est renforcée par le fait qu'il est possible, sur les blockchains, d'exécuter des *smart contracts* de manière à automatiser le partage des données. La technologie blockchain peut donc avant tout donner aux utilisateurs davantage de contrôle sur le partage de leurs données personnelles tout en assurant la portabilité de ces données. À cet égard, la technologie blockchain peut contribuer à garantir l'autonomie personnelle au sens du droit d'une personne de contrôler ses données personnelles et le traitement de ces données, comme le prévoit le Préambule de la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* (Convention 108).

La blockchain est déjà utilisée pour partager des données entre partenaires. Parmi de nombreux exemples, on peut citer la *Blockchain Insurance Industry Initiative* (B3i), qui permet aux plus grands assureurs du monde de partager des données sur les contrats d'assurance contre les catastrophes naturelles. Cette plateforme de partage de données permet aux participants (comme les assureurs, réassureurs et courtiers) de gérer tous les échanges administratifs, de la souscription au règlement des primes et des sinistres. Il s'agit d'une blockchain de consortium à permission dans laquelle les données traitées sont liées à une activité commune (par exemple, l'assurance contre les catastrophes naturelles) et où l'accès aux données est limité à un petit nombre de personnes. B3i a récemment été choisi par une coalition de pools nucléaires

européens pour développer une solution basée sur la blockchain pour la gestion des contrats de réassurance au sein de la coalition.

Il est également possible de créer des architectures ouvertes qui protègent les données personnelles des individus. Comme expliqué précédemment à propos des identités décentralisées, la blockchain permet de concevoir des méthodes de gestion et de partage des données tout en permettant aux utilisateurs de contrôler leurs propres données. Les utilisateurs peuvent utiliser leur clé privée pour autoriser ou refuser à des tiers l'accès à leurs données. Une blockchain connectée à une base de données hors chaîne stockant les données de l'utilisateur sous forme cryptée (à l'aide de clés de cryptage appartenant à l'utilisateur) stocke simplement un hash des données. Les conditions de partage des données entre les différents protagonistes sont prévues dans des *smart contracts*, et chaque accès reste soumis à l'accord de l'utilisateur. Un tel système garantit une transparence totale et assure que les données n'ont pas été modifiées, ni par l'utilisateur ni par quiconque. Les utilisateurs peuvent ainsi avoir un contrôle effectif sur l'utilisation de leurs données.

De nombreuses initiatives recourent à ces fonctionnalités, notamment dans le secteur de la santé. En Estonie, la technologie blockchain est utilisée pour donner aux patients un plus grand contrôle sur leurs données de santé. Chaque accès au dossier d'un patient et chaque modification de celui-ci peut être contrôlé grâce à la blockchain, qui garantit l'intégrité du système, des processus et des opérations. Ce sont les patients qui contrôlent et autorisent l'accès à leurs données de santé, y compris lorsque ceux qui les consultent sont des professionnels de santé. De même, le projet MyHealthMyData s'appuie sur une structure blockchain dans laquelle les personnes concernées peuvent autoriser, refuser et retirer l'accès à leurs données selon différents cas d'utilisation. L'objectif est de créer un registre à l'échelle européenne capable de recueillir les consentements de manière anonyme et de permettre l'accès aux données à tout moment, en tout lieu et par tout le monde. Les particuliers, les chercheurs, les laboratoires et les professionnels de santé pourraient facilement rechercher et mobiliser un grand volume de données tout s'assurant du consentement éclairé des patients, indépendamment de leur localisation, de la complexité des données et des lois régissant la protection des données. Aux États-Unis, Patientory utilise la blockchain pour organiser la consultation des dossiers médicaux et Medrec:M propose des solutions décentralisées de gestion des données de santé grâce à un registre d'authentification qui régit l'accès aux dossiers médicaux. Tout ceci pourrait déboucher sur des possibilités de partage à grande échelle où les dossiers médicaux pourraient être rendus accessibles et interopérables à tous les hôpitaux appartenant à un même réseau, ou à une même région.

Au-delà du secteur de la santé, la même approche pourrait être étendue à tous les domaines où il est nécessaire de partager des données personnelles. Par exemple, un consortium de quatorze organisations européennes a lancé le projet Decode, qui vise à fournir des outils permettant aux individus de contrôler l'utilisation de leurs données personnelles et non personnelles. Enfin, le projet Liberty vise à créer, grâce à la blockchain, des réseaux sociaux décentralisés et interopérables dans lesquels les utilisateurs sont les seuls maîtres de leurs données, grâce au protocole DSNP.

Références

DECODE (2020), DECODE : Giving people ownership of their personal data.

Fink, Michèle (2019), Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?, European Parliamentary Research Service.

MyHealthMyData (2020), A New Paradigm in Healthcare Data Privacy and Security.

Soutien aux réfugiés et aux populations vulnérables

La technologie blockchain pourrait aider à retracer et à documenter toutes les étapes des interventions en matière de migration et d'asile, notamment les procédures d'asile, les disparitions de migrants, les transferts de fonds et l'administration des grandes bases de données.

Compte tenu des fonctionnalités déjà évoquées permettant de gérer les identités, la technologie blockchain est de plus en plus considérée par les États, les entreprises et les défenseurs des droits de l'homme comme un outil de pointe pour assurer le respect des droits de l'homme et traiter les problèmes humanitaires les plus difficiles à résoudre, y compris ceux qui touchent de près les réfugiés, telle l'insécurité alimentaire.

Fournir une identité aux réfugiés

Selon la Banque mondiale, plus d'un milliard de personnes, dont 80 % vivent en Afrique subsaharienne et en Asie du Sud, ont des difficultés à obtenir un document d'identité officiel. En particulier, la plupart des 26 millions de réfugiés actuels ont perdu leurs documents d'identité originaux. Sans preuve d'identité, ces personnes ne peuvent pas accéder aux services de base tels que l'éducation, les soins de santé, les services financiers, ni même trouver un logement ou un travail. Elles sont privées de leurs droits et marginalisées dans la société.

Les systèmes d'identités décentralisées basés sur la blockchain pourraient résoudre les problèmes causés par les difficultés d'identification des populations vulnérables exposées au risque de discrimination ou d'exploitation, et leur permettre de bénéficier de manière effective de leurs droits les plus essentiels. Même sans documents d'identité officiels, les demandeurs d'asile pourraient se référer aux attestations et certificats collectés tout au long de la procédure de demande d'asile dans le pays d'accueil. Les blockchains peuvent, en effet, permettre aux différentes organisations impliquées (les ONG, les pouvoirs publics) de communiquer entre elles avec certitude. La blockchain pourrait donc permettre une identification plus rapide et plus sûre en cas de flux migratoires massifs.

Pour cette raison, de nombreux projets visent à fournir une identité numérique aux migrants, aux réfugiés et aux personnes déplacées. L'alliance ID2020, soutenue par l'ONU et menée par Microsoft, Accenture et plusieurs agences onusiennes, a proposé un réseau collaboratif d'identification numérique fondé sur la blockchain pour fournir une identification légale à 1,1 milliard de personnes sans documents d'identité officiels dans le monde. Au Kenya, la plateforme blockchain BanQu a aidé des réfugiés somaliens à disposer d'une identité numérique permanente et vérifiable. De telles plateformes blockchain peuvent fournir une identification numérique et un certificat numérique de naissance ou de diplôme sur un seul système. En outre, l'utilisation de la technologie blockchain pour gérer ces pièces d'identité peut permettre aux différentes organisations, autorités et institutions de communiquer entre elles avec certitude. Elle peut également permettre une identification plus rapide en cas de flux migratoire, ou de séparation des familles. Cette technologie a en effet été proposée pour aider des enfants à retrouver leurs parents et suivre le processus de réunification des familles.

Lutte contre la traite des êtres humains, notamment des enfants

Le déploiement de registres d'identification ouverts peut aider à prévenir la traite des êtres humains. Le Bureau des Nations Unies pour les services d'appui aux projets (UNOPS) travaille actuellement en partenariat avec le World Identity Network et le Bureau des technologies de l'information et de la communication des Nations Unies pour piloter un projet de blockchain

qui aide à identifier les personnes ayant perdu leur identité légale et, ce faisant, contribue à la lutte contre la traite des enfants. Ce projet fait partie de l'initiative Blockchain for Humanity, annoncée lors du sommet humanitaire sur la blockchain à New York le 10 novembre 2017. Selon les statistiques des Nations unies, près de la moitié des enfants de moins de cinq ans dans le monde ne possèdent pas de certificat de naissance. Ces enfants sont littéralement « invisibles » pour les autorités ou les agences de développement qui conçoivent et mettent en œuvre des programmes sociaux. Les enfants sans papiers sont des proies faciles pour les trafiquants d'êtres humains, qui utilisent souvent de faux documents d'identité pour les transporter au-delà des frontières. La blockchain pourrait non seulement aider à attraper les trafiquants puisque les identités numériques des enfants sont stockées et suivies, mais elle pourrait également aider à sécuriser les données sur un registre immuable, rendant les tentatives de trafic plus traçables et évitables. De même, la société américaine Consensys a remporté un appel d'offres pour lancer un projet pilote d'identité numérique dans lequel les enfants tentant de franchir une frontière seraient obligés de scanner leurs pupilles ou leurs empreintes digitales, ce qui permettrait d'avertir automatiquement leurs responsables légaux par téléphone.

Gérer et distribuer les aides et les ressources

Les systèmes basée sur une blockchain pourraient permettre aux pouvoirs publics et aux organisations internationales de gérer et distribuer efficacement l'aide et les ressources, tout en améliorant la transparence et la responsabilité dans l'aiguillage des aides et la dépense des fonds dans les pays tiers. Il n'est pas toujours évident de savoir comment les organismes d'aide dépensent les fonds collectés. Ces financements peuvent ne pas être suivis ou correctement comptabilisés. Les procédures actuelles pour les prestations, droits et aides impliquent une quantité importante de frais de gestion et de contrôles de conformité. Les programmes gouvernementaux tels que la sécurité sociale, les retraites, les soins médicaux et l'aide nationale et internationale pourraient bénéficier grandement de la technologie blockchain. Un registre ouvert et décentralisé pourrait permettre aux réfugiés, aux parties prenantes et au public qui fournissent des fonds à ces organisations de contrôler les dépenses, de voir si et comment les bénéficiaires sont réellement aidés. Il pourrait permettre d'automatiser les processus de vérification de l'éligibilité et du versement des fonds, par exemple dans le cas de la distribution d'indemnités à des personnes touchées par une catastrophe naturelle majeure. En outre, la technologie blockchain pourrait garantir que les prestations parviennent aux bénéficiaires prévus et ne sont pas détournées.

Certaines blockchains ont permis avec succès la distribution d'aide aux réfugiés. Le Programme alimentaire mondial des Nations unies a soutenu le projet « *Building Blocks* », une plateforme blockchain visant à relever les défis de la distribution de l'aide aux réfugiés. La plateforme facilite les transferts de fonds et la livraison de l'aide alimentaire pour les réfugiés syriens en Jordanie. Elle a permis aux organisations de créer des comptes virtuels pour les réfugiés, d'y déposer mensuellement des sommes en espèces, et de s'assurer que les fonds ne sont perçus que par la personne visée. Les bénéficiaires scannent leur iris pour payer leurs achats dans un supermarché, et leurs données sont vérifiées par comparaison à une base de données gérée par les Nations Unies. Le programme a permis de réduire les coûts d'administration et d'offrir plus de sécurité et de transparence aux réfugiés bénéficiaires de l'aide. De même, le service d'immigration finlandais s'est associé à Moni pour fournir aux demandeurs d'asile des cartes de crédit prépayées pour lesquelles les transactions étaient gérées sur une blockchain. Chaque carte était liée à une identité numérique unique et permettait aux réfugiés de recevoir de l'argent et des salaires, ainsi que de payer des factures, sans même devoir disposer d'un compte bancaire ou d'une pièce d'identité.

Soutenir les personnes dépourvues de compte bancaire

Les applications fondées sur la blockchain pourraient aussi venir en aide aux personnes n'ayant pas de compte en banque. La fondation à but non lucratif, Stellar Development, œuvre actuellement à donner accès aux services financiers aux populations non bancarisées. Cette blockchain décentralisée compte des partenaires dans le monde entier et permet aux particuliers de transférer de l'argent de manière rapide, fiable et pratiquement sans frais. Au Venezuela, BitGive, plateforme blockchain consacrée au suivi des dons, a été utilisée par des organisations pour collecter et distribuer de l'aide humanitaire à des orphelins, à des hôpitaux et à des centres recueillant des animaux. En Ouganda, l'Humanity First Token, monnaie virtuelle adossée à la monnaie fiat nationale, permet de procurer des fonds et des moyens de paiement aux réfugiés pour qu'ils puissent acquérir de la nourriture, des panneaux solaires et d'autres biens essentiels auprès de fournisseurs locaux. En Sierra Leone, Kiva, organisation à but non lucratif spécialisée dans la microfinance, œuvre en collaboration avec les Nations Unies et le gouvernement sierra-léonais avec l'ambition d'offrir à chaque citoyen du pays une identité basée sur une blockchain décentralisée qui donne accès à des services financiers. Kiva travaille au déploiement d'une plateforme d'identité fondée sur la blockchain, qui permettra aux personnes de construire un dossier de crédit à partir de leurs interactions passées avec les banques et les organismes de microcrédit. Chaque personne stocke dans son portefeuille les certificats remis par les institutions qui ont déjà eu des interactions avec elle. Lorsqu'elle prétend à un nouveau financement, elle peut donner à l'organisme de crédit visé l'accès à ces certificats.

Assurer le respect des droits des travailleurs

La blockchain peut aussi aider les réfugiés à voir leurs droits de travailleurs respectés, de manière juste et équitable. Les contrats de travail des réfugiés, ainsi que les différents accords relatifs à leur emploi pourraient être gérés par des *smart contracts*, évitant ainsi à ces travailleurs ce qu'ils subissent trop souvent : atteintes aux droits de l'homme ou exploitation par des multinationales ou les employeurs locaux. Ces *smart contracts* pourraient assurer le respect du droit du travail. Par exemple, des réfugiés syriens dans les zones rurales du Liban ont attribué leur incapacité à acheter de la nourriture au faible revenu qu'ils recevaient de leur travail, qui se déroulait dans des conditions purement informelles. Ils ont fait valoir qu'ils étaient fort peu payés pour leur travail et que leurs employeurs ne respectaient pas toujours l'accord informel initialement convenu. Or ils ne pouvaient pas faire appel à la justice, faute de contrat expressément dressé. Dans ce genre d'hypothèse, les *smart contracts* permettraient de garantir que les travailleurs reçoivent la juste rémunération qui leur est due. Un oracle pourrait fournir automatiquement l'heure de pointage du travailleur à un *smart contract* qui déclencherait le paiement immédiat du salaire du travailleur.

Limites et effets pervers du recours à la blockchain

Bien que garantissant transparence et responsabilité, l'utilisation des technologies blockchain peut également avoir des effets négatifs. L'intérêt général de la technologie pour aider les populations vulnérables doit être relativisé. Utiliser la blockchain pour identifier les personnes implique que les personnes concernées soient correctement équipées, notamment de téléphones intelligents et d'une connexion Internet. Or les populations les plus vulnérables ne le sont pas toujours. Ces problèmes d'accès aux appareils et à Internet ont déjà conduit certaines ONG à abandonner des projets pilotes d'identités décentralisées (SSI) en raison des difficultés rencontrées. Par conséquent, certains experts ont minimisé et relativisé l'intérêt d'utiliser les SSI comme outil d'autonomisation des groupes marginalisés. En outre, le stockage des clés privées des utilisateurs reste une question sensible, car celles-ci doivent être sécurisées de

manière adéquate et individuelle, étant donné qu'il est quasiment impossible de récupérer des clés perdues. Compte tenu de ces limites, il ne faut pas conclure que la technologie blockchain sera en mesure de compenser entièrement l'absence ou la perte de documents d'identités officiels dans un avenir immédiat.

De plus, comme pour toutes les solutions technologiques utilisées pour gérer les données, les risques en matière de protection de la vie privée sont bien présents, car non seulement les actions et les mouvements des individus peuvent être tracés, mais aussi parce que la technologie repose souvent sur des solutions privées ou développées par des entreprises. Même si les données personnelles sont chiffrées, l'enregistrement des transactions est visible par toute personne ayant accès à la blockchain. Cela peut être assez délicat et sensible pour des populations vulnérables comme les réfugiés apatrides. Dans le cas de la distribution d'aide, le fait que les transactions puissent être vérifiées pour s'assurer que l'argent est utilisé à des fins productives telles que le logement ou la nourriture, plutôt que l'alcool ou la drogue, implique un manque de confiance qui peut être dégradant pour le bénéficiaire. Dans le cas du versement de salaires, les blockchains pourraient être utilisées par les autorités pour prouver l'exercice illégal d'une activité à l'encontre des réfugiés et des migrants dont la situation n'est pas régularisée.

Références

Ardittis, Salon (2018), How Blockchain Could Make Refugee Programs More Transparent.

Bajpai, Prableen (2017), How Blockchain Can Help Humanitarian Causes.

Bureau des Nations Unies pour les services d'appui aux projets (2017), World Identify Network and United Nations team up to launch innovation blockchain pilot to help prevent child trafficking.

Cheesman, Margie (2022), Self-Sovereignty for Refugee? The Contested Horizons of Digital Identity, *Geopolitics* 27 : 1, 134–159.

Crumpler, William (2021), The Human Rights Risks and Opportunities in Blockchain, Center for Strategic and International Studies.

Gramatikov, Martin (2017), Unchaining Access to Justice: The Potential of Blockchain.

Irrera, Anna (2017), Accenture, Microsoft team up on blockchain-based digital ID network.

Orcutt, Mike (2017), How Blockchain is Kickstarting the Financial Lives of Refugees, *MIT Technology Review*.

Programme alimentaire mondial (2018), Building Blocks: Blockchain network for humanitarian assistance—Graduated Project.

Rueckert, Christian (2019), Cryptocurrencies and fundamental rights, *Journal of Cybersecurity*, 5 : 1.

Stellar Development Foundation (2018), Finance with a Mission.

Schrepel, Thibault (2019), Blockchain and human rights: utopia, or dystopia, or both?.

Talhouk, Reem, Kyle Montague & Andy Garbette (2018), Blockchain for Refugees: Current Uses, Opportunities and Considerations.

Wojno, Marc (2021), Binance calls for global regulatory frameworks for crypto markets: Released 10 Fundamental Rights.

Lutter contre les atteintes aux droits de l'homme sur les chaînes d'approvisionnement

Les clients de grandes entreprises ignorent souvent totalement les infractions et les atteintes aux droits de l'homme commises par les fournisseurs de ces entreprises. Ce phénomène est observé dans de nombreux secteurs, de la production alimentaire à l'extraction de diamants. Outre les violations des droits de l'homme, les clients ignorent comment fonctionnent les chaînes d'approvisionnement des produits et ne peuvent savoir si ce qu'ils mangent a été produit de manière éthique.

Les blockchains pourraient permettre aux clients et aux parties prenantes des chaînes d'approvisionnement de contrôler les pratiques des fournisseurs. En effet, elles offrent des opportunités uniques pour répondre à la fois aux problèmes de transparence et de traçabilité des chaînes d'approvisionnement avec la création d'un registre commun et de confiance relatif à la provenance des produits et les conditions de leur production à toutes les étapes de l'approvisionnement. Cela améliorerait la transparence tant pour le client que pour tous les acteurs de la chaîne d'approvisionnement, en les aidant à faire preuve d'une diligence raisonnable et à remédier aux violations des droits de l'homme. Cela permettrait également de rendre les acteurs plus responsables grâce à l'enregistrement des certifications de tiers et à la facilitation des audits en matière de respect des droits de l'homme, de conditions de travail et de préoccupations environnementales.

Par exemple, devant les appels des clients à plus de transparence, Everledger a lancé en collaboration avec des joailliers une plateforme blockchain permettant de retracer tous les aspects de la production de diamants. Lorsqu'ils achètent un diamant, les clients peuvent vérifier qu'il a été produit de manière durable. Provenance, entreprise siégeant au Royaume-Uni, utilise la blockchain pour retracer l'origine et le parcours des produits. Toutes les personnes intéressées peuvent télécharger l'application mobile Provenance pour connaître l'historique de leurs achats. En France, l'industrie agro-alimentaire a développé une blockchain assurant la traçabilité de la production de poulet. Dans le même esprit, le WWF a mis au point, en collaboration avec des entreprises de pêche, une plateforme utilisant la blockchain pour suivre la provenance du thon.

La blockchain ne peut pas éradiquer les pratiques déloyales sur le marché mondial, mais elle permet au public d'accéder à l'information. Plus le grand public connaîtra les circonstances dans lesquelles les achats se déroulent, plus les personnes seront en mesure de faire des choix éclairés.

Références

Commandré, Ysé, Catherine Macombe & Sophie Mignon (2021), Implications for Agricultural Producers of Using Blockchain for Food Transparency, *Sustainability* 2021, *13*, 9843.

Crumpler, William (2021), The Human Rights Risks and Opportunities in Blockchain, CSIS.

Project Provenance Ltd. (2018), Create and publish engaging, trustworthy sustainability content.

Tholen, Jerwin, Dennis de Vries, Audrey Daluz, Claudiu-Cristi Antonovici & Wietse Van Brug (2019), Is there a role for blockchain in responsible supply chains?, OECD Centre for Responsible Business Conduct.

Walport, Mark (2015), Distributed Ledger Technology: beyond block chain, UK Government Office for Science.

Protéger les titres fonciers et la propriété immobilière

Dans le domaine de l'immobilier, les registres fonciers sont essentiels pour assurer le droit à la propriété privée — de la gestion du cadastre à l'enregistrement des changements de propriétaire. Ces registres peuvent cependant être détruits par des cyberattaques ou des catastrophes naturelles. En conséquence, les propriétaires seraient privés des moyens légaux de faire valoir leurs droits, étant donné que les autorités ne disposeraient d'aucune trace des titres fonciers et de la propriété antérieure. Cela impliquerait également que les propriétaires n'auraient aucun moyen de prouver qu'ils ont droit à une indemnisation en cas de dommages. Même en l'absence de catastrophes, les registres fonciers sont parfois très précaires dans certaines régions du monde, en raison d'une administration défaillante, de la mauvaise tenue des registres ou de la corruption des autorités. Certains groupes marginalisés font l'objet d'une attribution inéquitable ou discriminatoire des terres, tandis que certaines communautés ont des difficultés à faire valoir leurs droits sur des terres ancestrales.

La technologie blockchain pourrait être exploitée pour fournir un registre sécurisé et transparent pour les titres fonciers, qui serait protégé contre les falsifications, les catastrophes et les abus. Elle pourrait améliorer la résilience des registres et garantir les droits des propriétaires privés, notamment en garantissant que les terres appartenant à des groupes marginalisés ne sont pas cédées sans leur consentement. Elle pourrait également permettre des gains d'efficacité et réduire les coûts associés aux transactions foncières et à la tenue des registres.

Au Ghana, la start-up Bitland a proposé de protéger les titres fonciers en conservant les actes de propriété sur un registre public soutenu par une blockchain. Il suffirait de consulter l'historique stocké sur la blockchain pour résoudre les litiges fonciers, ce qui éviterait les erreurs humaines et la perte de registres. L'Inde, la Géorgie, l'Ukraine et la Suède ont également entrepris de mettre en œuvre de telles structures pour faciliter la gestion des titres fonciers et la vente des biens immobiliers : une application sur blockchain enregistre toutes les informations détaillées sur les propriétés vendues, ainsi que chaque étape de la vente.

Références

Center for Social Innovation (2019), Blockchain for Social Impact: Moving Beyond the Hype, *Stanford Business*.

Crumpler, William (2021), The Human Rights Risks and Opportunities in Blockchain, CSIS.

Eder, Georg (2019), Digital Transformation: Blockchain and Land Titles, OECD Global Anti-Corruption & Integrity Forum.

Kim, Christine (2021), Sweden's Land Registry Demos Live Transaction on a Blockchain.

Nimfuehr, Marcell (2017), Blockchain application land register: Georgia and Sweden leading.

Oprunenco, Alexandru & Chami Akmeemana (2018), Using blockchain to make land registry more reliable in India.

Permettre l'exercice du droit de vote et la transparence démocratique

Les technologies blockchain présentent le potentiel voulu pour créer de nouvelles méthodes de vote, qui feraient évoluer à la fois les processus sur papier — encore très fréquents — et les processus électroniques n'ouvrant que de faibles possibilités de validation et d'audit. Pour les citoyens, ces méthodes seraient plus commodes et inspireraient davantage confiance. En garantissant que les votes individuels sont admissibles et comptabilisés correctement, les blockchains peuvent aider à prévenir les problèmes liés au processus électoral telle la falsification des bulletins, qui persiste dans de nombreux pays. Ces problèmes, s'ils ne sont pas résolus, peuvent entraîner un manque de confiance dans les processus démocratiques et permettre des résultats électoraux qui ne reflètent pas les souhaits du peuple.

Les caractéristiques principales de la technologie blockchain permettent de donner davantage de pouvoir démocratique aux citoyens grâce à la décentralisation et la diffusion de l'autorité. Cette autonomisation des citoyens peut être réalisée par le biais de blockchains où les membres prennent part aux processus de prise de décision : c'est une nouvelle forme de démocratie directe.

La blockchain et les outils logiciels qui l'accompagnent peuvent offrir aux États des fonctionnalités leur permettant d'organiser des élections de manière sécurisée et transparente, en garantissant l'authenticité de chaque vote exprimé et en s'assurant que le décompte des voix est exact. Le résultat d'une élection peut être fortement influencé par l'absence de liste électorale fiable. Le passage à un système de vote sur blockchain pourrait aider à prévenir la fraude électorale, car les blockchains sont cryptées, décentralisées et incorruptibles. Un tel système ne pourrait pas être corrompu par une seule partie, dès lors que le registre n'existerait pas en un seul endroit. En outre, sur une blockchain, les signatures pourraient être collectées et enregistrées numériquement, de manière immuable, ce qui réduit encore la possibilité de fraude. Une telle urne numérique sécurisée pourrait être adoptée par les organisations, les partis politiques et les entreprises du monde entier, augmentant ainsi la participation du public au processus démocratique grâce à des modalités de vote plus accessibles.

Les plateformes blockchain ne permettraient pas seulement de voter pour des partis politiques, mais aussi de participer davantage au processus législatif. Les signatures numériques pourraient être utilisées en vue d'introduire de nouveaux projets de loi dans les parlements. En 2016, l'Institut pour la technologie et la société de Rio de Janeiro (ITS Rio) a développé une application basée sur la blockchain appelée Mudamos qui établit l'identité des électeurs, sur la base d'un numéro d'identification unique que chaque électeur et contribuable brésilien reçoit de l'État. Cette application leur permet ensuite d'exprimer officiellement leur soutien aux projets et propositions de loi. Deux mois après son lancement, 600 000 personnes avaient téléchargé Mudamos. 7 000 propositions de loi ont été reçues à ce jour. La blockchain peut ainsi permettre de répondre à la forte demande en faveur d'une participation plus effective des citoyens à la vie publique.

Les blockchains ouvertes pourraient aussi accroître la transparence et l'esprit de responsabilité des partis politiques en matière de financement et de déroulement des campagnes électorales. Cependant, il existe un risque que la technologie blockchain soit réputée illégale ou réglementée par les autorités en place, en particulier si celles-ci sont corrompues. Ces risquent rendent encore plus nécessaire l'intervention de ceux qui cherchent à prévenir les violations des droits de l'homme et autres abus.

Enfin, si les blockchains sont efficaces pour assurer la sécurité, l'exactitude et la transparence du vote électronique et des activités démocratiques, certains facteurs peuvent entraver leur acceptation par le grand public ou leur déploiement efficace sur le terrain, tel le manque de culture numérique des populations ou de faibles possibilités de connexion.

Références

Biehl, Zoe (2018), 6 Ways Blockchain is Radically Improving Global Human Rights.

Boucher, Philip, Susana Nascimento & Mihalis Kritikos (2017), *How blockchain technology could change our lives*, European Parliamentary Research Science.

Chaum, David, et al. (2016), *The Scantegrity Voting System and its Use in the Takoma Park Elections*, Auerback Publications.

Hughes, Kobina (2017), Blockchain, the Greater Good, and Human and Civil Rights, *Metaphilosophy* 48 : 5 654-665.

ITS Rio, Mudamos.

Ledger Insight (2020), Russia's blockchain voting site crashes soon after it went live.

Ledger Insights (2021), Korea to trial blockchain in large scale online voting.

Lemos, Ronaldo (2016), Using the Blockchain for the Public Interest.

Nasser, Yomna, Chidinma Okoye, Jeremy Clark & Peter Y A Ryan (2018), *Blockchains and Voting: Somewhere between hype and a panacea (A Position Paper)*.

Zambrano, Raul, Ruhiya Kris Seward & Phet Sayo (2017), *Unpacking the disruptive potential technology for human development*, International Development Research Centre.

Fournir des solutions de règlement des litiges

La blockchain a déjà permis de développer des solutions de résolution de conflits grâce à des procédures d'arbitrage encodées dans des *smart contracts*. Les *smart contracts* peuvent en effet permettre l'exécution des décisions de résolution de conflits en ligne. Certaines plateformes offrent ainsi des services de « justice décentralisée » reposant sur des *smart contracts*. Les litiges découlant d'un accord ou liés à celui-ci sont résolus par des adjudicateurs privés au moyen de décisions qui s'exécutent automatiquement. La procédure suivie est entièrement automatisée, sans aucun contrôle humain.

Les principales plateformes sont Kleros, Aragon et Jur. La plateforme Aragon a mis en place un système de résolution des litiges particulièrement original qui fait intervenir des « gardiens ». Toute personne souhaitant porter un litige sur la plateforme verse un dépôt de garantie — qui lui est restituée en cas de victoire — et présente ses arguments. Les utilisateurs qui souhaitent jouer le rôle de « gardien » dans la résolution du litige doivent envoyer des jetons grâce au *smart contract* de l'« Aragon Court ». Plus un candidat a envoyé de jetons, plus la probabilité d'être sélectionné et de devenir « gardien » est élevée. Lorsqu'un utilisateur est sélectionné pour trancher un litige, une partie des jetons qu'il a envoyés est bloquée jusqu'à ce que le litige soit résolu. Contrairement aux tribunaux traditionnels, les « gardiens » de l'« Aragon Court » ne sont pas censés statuer de manière impartiale sur les litiges, mais bien plutôt en référence à ce que devrait être la décision probable d'un groupe de personnes ainsi sélectionnées. Pour encourager le consensus, les « gardiens » minoritaires, donc qui n'ont pas voté en faveur de la solution finalement adoptée, perdent leurs jetons. Quant aux « gardiens » majoritaires, qui ont voté en faveur de la solution finalement adoptée, ils sont récompensés : on leur verse les frais de litige payés par les parties ainsi que les jetons des « gardiens » ayant voté avec la minorité.

S'il existe ainsi un fort potentiel d'automatisation de la résolution des litiges et de l'exécution des décisions, se pose toutefois la question fondamentale de savoir comment préserver l'équité et la régularité des procédures au sein de ces réseaux décentralisés échappant au contrôle de l'État. Cela étant précisé, aucune raison ne justifie d'écarter a priori les solutions fondées sur la blockchain dans le cadre de la résolution des conflits. En particulier, les tribunaux traditionnels ne sont pas adaptés aux petits litiges transnationaux. À mesure que la technologie se développe, elle apparaît, à cet égard, de plus en plus adaptée pour régler les problèmes d'accès à la justice.

Vitalik Buterin, le cofondateur d'Ethereum, est sans surprise un partisan de l'utilisation de l'arbitrage fondé sur les *smart contracts*. Toutefois, il ne pense pas que cette solution puisse sérieusement remplacer les tribunaux traditionnels. Il estime que la blockchain concurrence avant tout les solutions existantes d'arbitrage privé. Pour lui, « les tribunaux traditionnels remplissent une fonction très importante, celle de déterminer quel est le recours approprié lorsque les parties à un litige n'ont aucune relation préalable, et qu'elles n'ont donc pas convenu d'un arbitrage entre elles » [traduction]. En outre, même si l'introduction d'une action en justice est susceptible d'être considérée comme disproportionnée compte tenu de la faible valeur de la majorité des litiges, l'exécution automatisée des décisions n'est possible que pour les biens et les transactions en ligne. Les États conservent le monopole de l'usage de la force sur les actifs numériques qui sont hors de portée des *smart contracts* et sur les actifs non-numériques. Ils ont également la responsabilité de traiter des conséquences du non-respect d'une décision de justice, qu'il s'agisse des jugements rendus par un tribunal étatique ou des sentences arbitrales.

Pour autant, la blockchain pourrait profiter à la justice. Dans la plupart des pays, la justice a un énorme problème de gestion de l'information. Les systèmes judiciaires disposent trop souvent de données de mauvaise qualité, qu'ils doivent en outre gérer à l'aide de systèmes et de processus hérités du passé. Or, des solutions fondées sur la blockchain ont déjà contribué à résoudre ce type de problèmes pour des entreprises et des activités financières. Les solutions blockchain pourraient offrir aux systèmes judiciaires l'occasion unique de renforcer l'exactitude et la transparence de leur activité au moyen de registres sûrs, auditables et distribués.

Enfin, dans tous les pays, mais surtout dans ceux où la corruption est préoccupante ou dans lesquels les forces de l'ordre et les systèmes judiciaires ont perdu la confiance du public, la technologie blockchain pourrait être mise à profit pour sécuriser les modes de preuve. Certains pays, comme la Chine, ont annoncé qu'ils envisageaient de développer des registres blockchain pour tracer les preuves médico-légales. De même, certaines entreprises ont proposé des outils aux forces de l'ordre, telle que Kinesense, plateforme d'enquête par vidéo, qui exploite la blockchain pour sécuriser les preuves numériques en allant du simple enregistrement à la création de rapports. Le hachage des preuves numériques permet de confirmer l'authenticité de tout élément de preuve utilisé et même de le tracer.

Références

Koulu, Riikka (2016), Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement, SCRIPTed 13:1 40.

Redman, Jamie (2016), Vitalik Buterin : Blockchain and the Future of Courts.

3. Questions juridiques soulevées par les technologies distribuées

Dans la perspective crypto-anarchiste libertarienne qui inspire les blockchains depuis l'origine, la technologie est destinée à se développer en dehors de tout contrôle centralisé, et donc en dehors de toute régulation étatique. En d'autres termes, pour ses promoteurs, la blockchain vise à établir un « ordre sans droit », régulé uniquement par le code informatique. De fait, certains des systèmes mis en œuvre aujourd'hui peuvent donner l'impression d'un ordre sans droit. Certains ont mis en place de véritables systèmes de régulation privée, automatisés et codés. Il a été soutenu que le déploiement généralisé des blockchains créerait l'apparition d'une nouvelle branche du droit appelée *lex cryptographia*. Certains partisans irréductibles de la technologie affirment que les systèmes cryptographiques sont plus difficiles, voire impossibles à réguler. Selon eux, les réseaux blockchain seraient la version ultime du « *code is law* » (le code est le droit), ce qui aurait pour effet de faire passer la société du règne de la « règle de droit » ("*rule of law*") à celui de la « règle du code ».

Cependant, cette perspective n'est pas tenable pour le juriste ou le régulateur, et elle s'est révélée fausse dans le monde entier. Si nous disposons aujourd'hui d'algorithmes puissants pour mener à bien certaines tâches, il se trouve des humains derrière ces algorithmes, ne serait-ce que pour les développer. Et on ne laisse pas les algorithmes prendre seuls toutes les décisions. C'est pourquoi, en tant que société, il vaut mieux s'abstenir de simplifier à outrance la réflexion sur la technologie et s'attaquer plutôt aux problèmes réels soulevés par l'innovation.

Or la blockchain suscite des questions juridiques complexes, qu'il s'agisse de la protection de l'anonymat et du droit à la vie privée, du statut juridique des contrats automatisés et des organisations autonomes décentralisées, ou encore des conflits de lois et de juridictions dus à la nature distribuée et transnationale de la plupart des applications.

Risques en matière de protection des données personnelles

Comme indiqué précédemment, en dépit de la protection garantie par le pseudo-anonymat sur les plateformes blockchain, la transparence de la technologie présente des risques en matière de protection des données des utilisateurs. D'un point de vue juridique, elle pose certainement la question de sa compatibilité avec les règles de protection des données personnelles, dans la mesure où la technologie n'empêche pas toujours l'identification des utilisateurs concernés.

Les premiers projets de blockchain ont été conçus pour stocker indéfiniment les données, afin de faciliter leur intégrité et leur auditabilité. L'idée était que chaque transaction remontant au premier bloc (le « bloc de genèse ») reste indéfiniment dans le registre. À cet égard, la blockchain permet aux utilisateurs de stocker, d'authentifier et de sécuriser les données, leur conférant un caractère intangible et immuable. Toutefois, ces caractéristiques entrent en conflit avec les objectifs actuels de la protection des données personnelles, telles que la minimisation des données, la limitation du stockage, le droit de rectification, le droit d'opposition au traitement et le droit d'effacement des données.

En 2019, Michèle Fink a mis en évidence les nombreux points de tension entre la technologie blockchain et les principes issus du *Règlement général sur la protection des données* (RGPD). Le RGPD repose sur l'hypothèse qu'il existe toujours un « responsable du traitement » auquel les personnes concernées peuvent s'adresser pour faire valoir leurs droits en matière de

protection des données. Cependant, la nature décentralisée des blockchains rend très difficile l'identification de tels responsables. En outre, le RGPD exige que les données puissent être modifiées ou supprimées. Or, les caractéristiques de la technologie blockchain rendent la suppression ou la modification impossible, ou du moins très difficile. Il est certain que les concepts juridiques du RGPD présentent des incertitudes qui ne permettent pas toujours de tirer des conclusions précises sur la compatibilité de la technologie blockchain avec les principes de la protection des données personnelles.

Les points de tension identifiés à propos du RGPD sont également problématiques et préoccupants au regard d'autres textes encadrant la protection des données. Les caractéristiques de la blockchain entrent plus particulièrement en conflit avec les principes découlant de la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* (Convention 108). Deux caractéristiques clés de la technologie blockchain semblent particulièrement problématiques : la transparence et l'immutabilité. Comme indiqué précédemment, de nombreuses plateformes blockchain sont conçues dans un souci de transparence, de sorte que les transactions peuvent être vues par n'importe qui et que ceux qui les réalisent sont éventuellement identifiables. Cela présente des risques pour les utilisateurs, et une responsabilité potentielle pour les opérateurs de plateformes. En outre, le principe d'immutabilité qui garantit l'intégrité de la blockchain et évite les incohérences va à l'encontre des droits de rectification et d'effacement. En principe, toute tentative d'un utilisateur d'effacer ou d'écraser des données existantes sera détectée par les autres et corrigée. Cependant, même si un bloc existant ne peut être modifié, des alternatives existent et sont utilisées aujourd'hui, tel l'ajout d'une nouvelle transaction pour rectifier l'information. Dans ce cas, même si l'information initiale est toujours présente, les gens voient d'abord les données mises à jour. En outre, lorsque les données sont chiffrées, il est toujours possible pour la personne qui souhaite les effacer de détruire la clé de chiffrement. Une fois la clé détruite, les données deviennent indéchiffrables pour tout le monde, ce qui revient presque au même qu'un effacement — sous réserve que le chiffrement ne puisse pas être cassé.

Dans l'ensemble, les incompatibilités avec les règles relatives à la protection des données personnelles méritent néanmoins d'être nuancées compte tenu de la grande variété des plateformes blockchain existantes et de leurs caractéristiques techniques distinctes. Par exemple, des techniques sont en cours de développement pour renforcer la confidentialité et l'anonymat et pour donner aux utilisateurs plus de contrôle sur leurs données. Certaines plateformes ne permettent qu'aux utilisateurs autorisés d'accéder aux informations stockées sur la blockchain, d'autres sont conçues pour assurer le secret des transactions, préserver l'anonymat et limiter au maximum la transparence. Il faut noter que le stockage hors chaîne des données personnelles pourrait faire partie de la solution, puisque seules les données de transaction seraient sur la blockchain. Les données personnelles pourraient être stockées de manière sécurisée dans un serveur géré par un tiers sous le contrôle de l'utilisateur qui pourrait également les supprimer ou les modifier. Un tel système serait également souhaitable pour garantir que les utilisateurs qui ont perdu leurs clés privées puissent toujours récupérer leurs données. Il présente toutefois des risques en matière de sécurité, car un tiers pourrait prendre le contrôle des clés.

En définitive, il apparaît que l'objectif de protection des données personnelles doit avant tout être pris en compte par les développeurs qui conçoivent l'architecture des plateformes blockchain. Ils devront veiller à ce que les modes de gouvernance et les opérations réalisées sur les blockchains soient établis de manière à ce que la protection des données soit garantie.

Références

Commission Nationale de l'Informatique et des Libertés (2018), Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles ?

Fink, Michèle (2019), Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?, European Parliamentary Research Service.

Rueckert, Christian (2019), Cryptocurrencies and fundamental rights, *Journal of Cybersecurity*, 5 : 1.

Conflits de lois et de juridictions

L'un des plus grands défis juridiques pour les systèmes blockchain est la détermination de la loi applicable et de la juridiction compétente compte tenu de la nature distribuée de la technologie. Bien que cet enjeu de la détermination de la juridiction et de la loi applicable pour les réseaux globaux, tel qu'Internet, ne soit pas nouveau, la technologie des registres distribués ne fait qu'accentuer le problème. Alors que, pour un site Internet, la localisation des parties, des serveurs ou de l'accessibilité d'un service peut être établie, il n'en va pas de même pour les applications sur la blockchain. Sur une blockchain, le contenu et les transactions peuvent passer par des nœuds et des opérateurs réalisant des transactions dans le monde entier et dans de nombreux États. Ces nœuds peuvent à tout moment se trouver dans n'importe quel pays, et de nouveaux acteurs peuvent rejoindre ou quitter le réseau à tout moment depuis n'importe où.

Dans un environnement entièrement distribué, il n'existe aucun lien substantiel précis pour identifier la loi applicable. Même si la loi applicable peut finalement être déterminée, cela s'accompagne d'une incertitude quant aux juridictions compétentes si rien n'a été convenu au départ. Bien sûr, il peut arriver que les parties aient pris soin d'inclure des dispositions concernant la loi applicable, ainsi que le choix du forum pour les litiges — par exemple par des commentaires dans le code du *smart contract*, de la DAO ou du NFT pourraient inclure de véritables dispositions contractuelles. Certains systèmes juridiques permettent aux parties de choisir une juridiction et une loi applicable s'il existe un lien substantiel avec le pays concerné. En raison du caractère distribué de la blockchain, il serait théoriquement possible pour une partie de choisir un forum dans un autre État, là où un nœud est opéré. En ce qui concerne le règlement des litiges, le contrat pourrait également inclure une clause compromissoire. Mais en l'absence d'une telle clause, la difficulté est d'autant plus grande qu'il peut être complexe de localiser les nœuds, ou d'identifier le serveur ou la personne physique ou morale responsable de l'administration de la plateforme. De plus, même lorsque les parties sont identifiées, l'application des règles traditionnelles n'est pas forcément aisée si elles sont géographiquement éloignées.

Comme souligné précédemment, il peut arriver que, même lorsque les parties n'ont pas conclu de contrat juridique au sens formel du terme, les modalités de règlement des litiges soient prévues dans des *smart contracts* par le code informatique de la plateforme. L'utilisation d'une « justice décentralisée » peut être très efficace et adaptée à l'économie de plateforme. Toutefois, ces méthodes très particulières de règlement des litiges doivent être utilisées dans le respect des droits des parties et de la légalité. Il est, par exemple, nécessaire que le mode de règlement des litiges en ligne proposé par la plateforme Aragon (présentée plus haut) respecte réellement les droits procéduraux des parties.

Dans tous les autres cas, la détermination des règles applicables et appropriées peut être un véritable casse-tête. Compte tenu du grand nombre de normes et de juridictions concurrentes, on pourrait soutenir qu'aucune ne devrait s'appliquer. On serait en présence de systèmes, de contrats et d'organisations sans loi, hors de toute compétence étatique. Tel est certainement ce

que les crypto-anarchistes recherchaient à l'origine de la technologie. Cependant, il ne s'agit pas d'une position tenable dans des États de droit, de même que l'on ne peut accepter l'approche consistant à pouvoir appliquer plusieurs droits concurrents. Il pourrait être approprié ici d'élaborer un ensemble de principes généraux — tels les principes de la CNUDCI ou d'Unidroit — pour régir la détermination de la loi applicable et de la juridiction compétente pour les réseaux distribués. Ces principes proposeraient également un cadre uniforme pour réglementer les plateformes blockchain avec un certain nombre de règles communes considérées comme essentielles (par exemple, l'information des consommateurs, les possibilités de modifications du registre, les recours, etc.).

Références

Guillaume, Florence (2019), Chapter 3: Aspects of private international law related to blockchain transactions, in Kraus, Daniel, Thierry Obrist & Olivier Hari (2019), *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law*, Edward Elgar Publishing.

Wright, Aaron & Primavera De Filippi (2015), Decentralized Blockchain Technology and the Rise of Lex Cryptographia.

Werbach, Kevin (2018), Trust, but Verify: Why the Blockchain Needs the Law, *Berkeley Technology Law Journal* 33 : 2 487.

Werbach, Kevin (2018), *The Blockchain and the New Architecture of Trust*, MIT Press.

« Contrats » intelligents (*smart "contracts"*)

L'introduction des « contrats intelligents » a soulevé des questions sur la façon dont ce dernier développement technologique se conforme à la doctrine contractuelle traditionnelle. Les *smart contracts* ne sont pas toujours des contrats au sens juridique : les conditions essentielles pour la conclusion d'un contrat peuvent faire défaut, ou alors certaines exigences formelles particulières n'ont pas été respectées. Cependant, les *smart contracts* pourraient révolutionner la pratique du droit des contrats et ils ne semblent pas en ébranler les fondements. En effet, les universitaires, les législateurs et les tribunaux discutent de la numérisation des contrats depuis des décennies. Les États ont modifié les dispositions relatives aux contrats dressés sur papier et adapté leurs législations pour les contrats conclus numériquement, notamment sur la base des principes de la CNUDCI. Par conséquent, les « contrats intelligents » peuvent facilement être articulés avec le droit des contrats, qu'il s'agisse de la *common law* ou du droit civil, même si cette pratique peut soulever des questions liées à leur exécution et à la juridiction compétente. Cela dit, de telles questions ne sont pas propres aux *smart contracts*, et découlent plutôt de l'ubiquité du contexte numérique.

Nature juridique

Si l'on garde à l'esprit que le *smart contract* n'est qu'un simple programme informatique, il peut être logique de le dissocier de l'accord des parties, et donc du contrat au sens juridique du terme. Même si le *smart contract* devait aboutir à la conclusion d'un accord au sens juridique, il ne peut pas toujours remplacer le contrat juridique. Il est facile de distinguer le contrat du *smart contract* lorsqu'un accord a été expressément conclu entre les parties avant la mise en œuvre et/ou l'exécution du *smart contract*. Dans ce cas, le *smart contract* ne correspond pas à l'accord lui-même, ni à l'expression de cet accord, qui a été conclu verbalement ou par écrit, fût-ce sous forme électronique. Il s'agit simplement d'un moyen d'exécution du contrat.

Cela dit, il est fréquent que les *smart contracts* ne fassent pas qu'exécuter un contrat juridique traditionnel préalablement conclu, mais qu'ils constituent la seule expression de la volonté des parties. Dans ce cas, ces *smart contracts* pourraient-ils être considérés comme des contrats au sens juridique ? Il est tentant de voir le *smart contract* comme l'expression du contrat liant les parties : c'est l'hypothèse du « *code-only smart contract* ». Le *smart contract* pourrait représenter et matérialiser l'accord conclu et servir à ce titre, de preuve de l'existence du contrat. Cependant, pour qu'un *smart contract* soit considéré comme un contrat ayant force obligatoire d'un point de vue juridique, il doit satisfaire à toutes les exigences d'un contrat valide.

Juridiquement, un contrat est un accord entre deux ou plusieurs personnes qui donne lieu à une obligation dont les tribunaux peuvent ordonner l'exécution forcée. Pour qu'un contrat soit valable, il doit y avoir une « rencontre des volontés » des parties sur les éléments essentiels du contrat.

Pour que la rencontre des volontés ait lieu et qu'un contrat soit contraignant, les principes du droit des contrats exigent une offre et une acceptation formelles, ainsi qu'une contrepartie et un objet appropriés. La réunion des éléments du contrat dans le contexte numérique, et notamment dans le cadre de transactions automatisées et désintermédiées, peut cependant présenter certaines difficultés. Néanmoins, il est possible de faire en sorte que ces conditions soient réunies électroniquement. Ainsi, si le *smart contract* comprend tous les éléments requis, il pourrait être considéré comme un contrat valide en droit. Les effets contractuels juridiquement contraignants de tels *smart contracts* dépendront d'un certain nombre de facteurs. On ne sait cependant pas, tant que les tribunaux ne sont pas penchés sur cette question, comment les parties à un *smart contract* pourront démontrer que chaque condition de formation de contrat a été satisfaite.

La question de savoir si les *smart contracts* sont, juridiquement, des « contrats » est d'autant plus aigüe lorsqu'on examine les conditions de la formation des contrats dans certains contextes spécifiques, notamment en présence d'une partie faible (par exemple, consommateurs ou emprunteurs) ou lorsque la loi prévoit une forme spécifique (par exemple, les actes notariés).

L'absence de conclusion d'un contrat au sens traditionnel avant la mise en œuvre du *smart contract* peut par ailleurs poser un problème de preuve. Le *smart contract* peut être juridiquement insuffisant dans les cas où une forme spécifique est requise à des fins probatoires, et où la loi applicable exige un contrat écrit. Dans ce cas, le code informatique seul, même si les parties ont clairement consenti à son application, ne peut être juridiquement considéré comme équivalent à un accord écrit et ne sera valable — si tant est qu'il le soit — que comme un simple commencement de preuve. Il en sera de même dans les cas où le respect d'une forme spécifique est exigée comme condition substantielle. Dans tous ces cas, il sera nécessaire de rédiger au préalable un contrat classique, soit avec un document papier, soit avec des formulaires prévus pour la conclusion d'un contrat sous forme électronique.

Automatisation et immutabilité

Au-delà de la simple question de la nature juridique des *smart contracts*, l'immutabilité et l'automatisation qui les caractérisent, qui ne laissent aucune marge de manœuvre aux parties, peuvent comporter des risques. En effet, il est impossible d'empêcher l'exécution automatique du *smart contract*. Comme le programme peut être exécuté de manière continue, il est important d'être extrêmement prudent lors de sa programmation. Si une transaction est prévue, elle sera répétée en boucle. S'il y a une erreur, elle le sera également.

En outre, l'immutabilité de la blockchain empêche toute modification et toute adaptation des termes du contrat en cas, par exemple, de changement de circonstances. De ce point de vue, la

technologie du *smart contract* pousse à l'extrême la célèbre maxime *pacta sunt servanda* (« les accords doivent être respectés »). Toutefois, l'impossibilité de modifier la programmation peut également présenter des difficultés. La modification des *smart contracts* qui ne sont pas programmés pour être modifiés pourrait s'avérer nettement plus difficile et coûteuse qu'elle ne l'est actuellement pour des contrats modifiés par la conclusion d'un avenant. Contrairement aux pratiques habituelles de modification des contrats, il n'est pas possible de modifier quoi que ce soit dans les termes du *smart contract* — à moins qu'une telle possibilité soit incluse dans la programmation d'origine. Dans le même temps, un *smart contract* qui ne peut pas être modifié peut être considéré comme nul dans certains pays ou secteurs d'activité.

La seule solution est de prévoir dès le départ, dans la programmation, la possibilité de modifier le *smart contract*, d'accorder un délai de grâce ou même de renoncer à l'exécution du smart contract. Ce n'est cependant pas facile, car toute programmation nécessite des clauses extrêmement précises. Si la possibilité de modifier le contrat est programmée, les conditions dans lesquelles la modification peut avoir lieu et les changements possibles doivent tous être détaillés. Dans le cas contraire, la modification du *smart contract* est quasiment impossible. Parfois les parties pourront se mettre d'accord sur un nouveau *smart contract* qui corrige l'effet du premier: par exemple un nouveau *smart contract* permet à un débiteur défaillant d'accéder à nouveau aux objets connectés dont il est privé du fait de sa défaillance. Toutefois, cette solution est difficile à mettre en œuvre en présence de *smart contracts* qui s'adressent à plusieurs utilisateurs qui ne sont pas toujours identifiables en raison de la pseudo-anonymisation.

Cette immutabilité des *smart contracts* peut également entrer en conflit avec certains principes essentiels du droit des contrats, tels que les principes d'ordre public ou le devoir de bonne foi, qui sont imposés sous peine d'annulation ou de résolution du contrat. En droit civil et dans certains pays de *common law*, les parties doivent s'entendre et exécuter les contrats de bonne foi, sous peine de nullité. Puisque l'obligation de bonne foi s'applique à tous les contrats, elle doit s'appliquer aux *smart contracts* dès lors que ceux-ci sont effectivement des contrats. Cependant, la manière dont l'obligation de bonne foi pourrait s'appliquer à l'exécution des *smart contracts* n'a pas encore été étudiée. Au-delà de l'ordre public et de l'obligation de bonne foi, la question se pose également à propos de toutes les autres causes de résolution ou de nullité du contrat. Comment une partie pourrait-elle faire « annuler » un *smart contracts* alors qu'il est impossible de le modifier ? Il ne s'agit pas tant d'une question juridique que d'une question d'application du droit. Certes, on pourrait, dans certains cas, intégrer certains principes dans la programmation initiale et s'appuyer sur des oracles, même si, comme nous l'avons vu précédemment, le recours aux oracles comporte ses propres difficultés.

Encodage des termes juridiques et interprétation du code informatique

Malgré les perspectives ouvertes par les *smart contracts*, un problème majeur se pose : la viabilité des *smart contracts* exige la capacité d'exprimer les obligations contractuelles en code informatique. Le langage naturel ne pouvant être exécuté directement par un ordinateur, les *smart contracts* requièrent que les obligations contractuelles soient traduites en termes lisibles et exécutables par ordinateur. Cependant, cette conversion et l'exécution du code qui en résulte ne peuvent pas toujours être réalisées. En outre, traduire les contrats juridiques en code exécutable automatiquement implique de perdre une grande partie de la fonctionnalité et de la flexibilité du langage juridique traditionnel. Les mots « raisonnablement », « aux meilleurs efforts du vendeur », « cas de force majeure » ou « bonne foi », par exemple, sont difficiles à coder sous la forme « si ceci, alors cela ». De plus, en l'état actuel des choses, le code informatique ne fonctionne pas bien avec des dispositions qualitatives ou subjectives. Or de nombreuses obligations contractuelles dans les contrats actuels sont rédigées avec l'intention

d'être suffisamment génériques pour être applicables à une variété de situations différentes, dont certaines auraient pu ne pas être prévues au moment de la rédaction.

En outre, le fait de s'abstenir de rédiger un contrat au sens traditionnel en s'appuyant exclusivement sur un *smart contract* crée une difficulté dans la mesure où, pour pouvoir consentir à l'application du *smart contract*, encore faut-il pouvoir en comprendre les dispositions. Si aucune présentation des termes du *smart contract* n'est faite en langage courant, alors la partie qui n'a pas de compétences informatiques risque de ne pas pouvoir comprendre à quoi elle s'engage. Le problème est d'autant plus aigu que, dans la plupart des cas, les *smart contracts* sont des contrats standards dans lesquels un prestataire offre des services (par exemple, une couverture d'assurance) dans le cadre d'un *smart contract* déjà en place. Il est donc souhaitable que l'utilisation d'un *smart contract* s'accompagne de la divulgation préalable de toutes les explications et précisions nécessaires afin que les utilisateurs puissent donner leur consentement éclairé.

Il existe également un problème de responsabilité professionnelle pour les juristes qui peuvent ne pas comprendre les caractéristiques et les limites des logiciels informatiques. À l'inverse, les personnes formées en informatique ne sont généralement pas familières avec la portée et les subtilités des termes juridiques. Par conséquent, aucun des deux groupes n'est suffisamment compétent pour anticiper les problèmes qui peuvent survenir avec les *smart contracts* les plus avancés. Ou pour apprécier ce qu'ils ne savent pas. Cette difficulté a des implications importantes pour la programmation d'un *smart contract*, car, de la même manière qu'une virgule dans un contrat peut coûter des millions, une faute de frappe dans un programme peut faire échouer une transaction ou la faire exécuter par erreur — ou coûter des millions.

Mise en œuvre et exécution

Dès lors qu'un *smart contract* est jugé juridiquement contraignant, la question de son exécution soulève de nouvelles questions. Compte tenu des possibilités d'exécution automatique des *smart contracts*, certains chercheurs ont vanté la capacité de ces contrats à éliminer les litiges en matière d'exécution forcée du contrat. La question de l'exécution forcée se pose lorsqu'une partie introduit une action en justice en raison du manquement de l'autre partie à ses obligations contractuelles et que la réparation recherchée est l'ordre d'exécuter les obligations concernées.

Tout l'intérêt du *smart contract* est que la question de l'exécution du contrat est réglée d'emblée, puisque l'exécution a lieu automatiquement dès que les conditions fixées par le programme sont remplies. Les *smart contracts* permettent de se passer de l'exécution forcée, puisque l'intervention humaine est supprimée ou limitée. Une limite notable de cet argument est que la blockchain ne peut pas physiquement exécuter un contrat, ni contraindre une personne ou une entité à s'acquitter de ses obligations, ce qui signifie que les tribunaux seront probablement amenés à se pencher sur les questions d'exécution dans un contexte nouveau.

Plus le *smart contract* est complexe, plus des litiges peuvent survenir en raison de problèmes de programmation, d'une exécution erronée, de la défaillance d'un tiers (par exemple, un oracle fournissant des données ou exécutant une action), de l'intention des parties et d'autres questions non techniques. Une solution consiste à inclure dans le *smart contract* un mécanisme de résolution des litiges qui permet aux parties de soumettre les problèmes à un tribunal ou à une juridiction arbitrale, qui pourrait alors décider de la manière de résoudre le litige.

L'absence d'un tel mécanisme ou oracle intégré ne prive pas les parties de leur droit à la justice, puisqu'elles peuvent toujours déposer une plainte devant une juridiction judiciaire. Certes, dans la mesure où un programme informatique ne peut pas être réécrit, un tribunal ne sera pas en mesure d'ordonner des mesures à exécuter sur une blockchain, ni d'imposer que le

code informatique soit défait. Toutefois, le tribunal conserve la possibilité d'ordonner aux parties d'atténuer les conséquences du *smart contract* (par exemple, écrire un nouveau *smart contract* qui annulerait l'exécution erronée, exécuter l'obligation ou dédommager les autres parties lorsque l'exécution forcée n'est pas possible).

Limites nécessaires

Bien que certains considèrent les *smart contracts* comme des instruments supérieurs aux contrats traditionnels, la technologie des *smart contracts* a sans aucun doute ses limites et soulève des difficultés juridiques importantes. Il est probable qu'à l'avenir, ces difficultés s'atténuent grâce à l'évolution de la technologie. Les projets actuels visent à développer des *smart contracts* qui peuvent être modifiés ou résolus. En outre, l'intégration de couches d'intelligence artificielle rendra les *smart contracts* encore plus « intelligents » en permettant au code de s'adapter en fonction de conditions moins précises et en laissant une marge d'appréciation à la machine.

Il ne serait pas réaliste de renoncer aux possibilités qu'offrent les *smart contracts* en termes d'automatisation et de réduction des coûts, d'autant que les entreprises les utilisent de plus en plus fréquemment. Cependant, il ne semble pas non plus acceptable de permettre que les *smart contracts* soient mis en œuvre et proposés aux utilisateurs en dehors de toute règle, garantie et recours, notamment lorsqu'il s'agit de consommateurs, de groupes marginalisés et de personnes ayant une faible culture numérique.

Références

Abrahams, Nick, Zein El Hassan & Sean Murphy (2016), Can Smart Contracts be Legally Binding Contracts? An R3 and Norton Rose Fulbright White Paper.

G'sell, Florence (2019), « Intelligence artificielle et blockchain », in Bensamoun, Alexandra & Loiseau, Grégoire (2019), *Droit de l'intelligence artificielle*, Dalloz.

Kolber, Adam (2018), Not-So-Smart Blockchain Contracts and Artificial Responsibility, *Stanford Technology Law Review* 21 : 2 199.

Lipshaw, Jeffrey (2018), The Persistence of 'Dumb' Contracts, *Stanford Journal of Blockchain Law & Policy* 2 : 1.

Martin-Bariteau, Florian & Marina Pavlović (2020), AI and Contract Law, in Florian Martin-Bariteau & Teresa Scassa (eds.), *Artificial Intelligence and the Law in Canada*, LexisNexis.

Martin-Bariteau, Florian & Marco Pontello (2020), *Hashing Out Agreements: An Overview of Smart Contracts under Canadian Law*.

Mik, Eliza (2017), Smart Contracts: Terminology, Technical Limitations and Real World Complexity.

Raskin, Max (2016), The Law and Legality of Smart Contracts, *Georgetown Law Technology Review* 1 : 2 305.

Sherborne, Andreas (2017), Blockchain, Smart Contracts and Lawyers, Association internationale du barreau.

Tjong Tjin Tai, Eric (2017) Formalizing Contract Law for Smart Contracts, Tilburg Private Law Working Paper Series 06 : 2017.

Nature juridique des organisations autonomes décentralisées

La capacité des programmes informatiques que sont les organisations autonomes décentralisées (DAO) à concurrencer des organisations pleinement fonctionnelles et autonomes soulève la question de leur nature juridique. Les DAO doivent-elles être considérées comme des lignes de code informatique ou le droit doit-il les reconnaître comme des personnes morales, ou quelque chose entre les deux ? La question de la reconnaissance de la personnalité juridique aux DAO est aujourd'hui posée par l'existence d'organisations de plus en plus intelligentes ayant la possibilité d'effectuer des transactions — et donc des actes juridiques — de manière purement automatisée. À la lumière des lois uniformes de la CNUDCI, la plupart des pays ont reconnu la possibilité de contracter avec un agent électronique par le biais des mécanismes juridiques de la représentation ou du mandat. Toutefois, les DAO nous invitent à réexaminer ces questions, car elles n'impliquent pas une seule personne, mais un groupe.

La nature contractuelle des DAO est indiscutable : en décidant d'acquérir des jetons DAO et de participer à son fonctionnement, les détenteurs de jetons expriment leur volonté de collaborer dans le cadre établi par le protocole informatique. À ce titre, une DAO pourrait être considérée comme une « organisation contractuelle », où les règles de gouvernance établies dans le code pourraient être considérées comme similaires aux articles ou aux statuts d'une organisation. Un certain nombre d'études invitent à considérer ces organisations comme des sociétés *de facto*, étant donné que le code impose la coopération et la conformité avec le schéma de gouvernance de l'organisation, ainsi que la qualité de membre des détenteurs de jetons. La *common law* et le droit civil ont appris à reconnaître les sociétés créées de fait, avec, dans certains cas, une responsabilité limitée pour leurs membres. Si nous considérons les DAO comme des organisations contractuelles, elles pourraient être reconnues comme des sociétés en nom collectif ou des sociétés en commandite dans les droits de *common law*, comme des sociétés en participation dans les pays de droit civil, ou comme des « tokumei kumiai » au Japon. L'entité serait reconnue comme une entreprise en soi dans laquelle toutes les parties prenantes seraient entièrement responsables, mais elle n'aurait pas la personnalité juridique.

À la lumière de ces discussions, Malte a élaboré un cadre permettant l'immatriculation et la reconnaissance juridique des DAO, sans toutefois leur accorder une pleine personnalité juridique. Par ailleurs, le Wyoming, le Vermont et le Delaware, ainsi que la République des Îles Marshall, ont prévu de nouveaux régimes d'immatriculation des sociétés reconnaissant les DAO comme un nouveau modèle de société à responsabilité limitée disposant de la personnalité juridique, ce qui permet de protéger les détenteurs de parts/de jetons. En général, ces législations exigent qu'une ou plusieurs personnes physiques, agissant en tant que membre ou représentant de la DAO, divulguent leur identité et leur lieu de résidence. La situation est toutefois beaucoup plus compliquée lorsque les créateurs et les participants de la DAO ne révèlent pas leur identité. Il semble difficile, dans un tel cas, de reconnaître la personnalité juridique d'organisations purement virtuelles créées ou animées par des personnes inconnues. Les tiers effectuant des transactions avec une telle entité n'auraient aucun recours en cas de problème.

Lorsque la personnalité juridique des DAO n'est pas reconnue par la réglementation applicable, les détenteurs de jetons pourraient également décider de créer une véritable société, tout en prévoyant dans les statuts que les règles et les décisions seront prises par la DAO. Cependant, non seulement cela suppose qu'une personne physique agisse en tant que mandataire de la société, mais l'organisation et le fonctionnement de la DAO doivent être

conformes au droit des sociétés. Bien que cette option apporte une certaine sécurité juridique, elle représente une contrainte très forte pour les détenteurs de jetons.

Il est important de noter que, lorsque cela est prévu par la réglementation applicable, la personnalité juridique des DAO est limitée dans ses capacités de la même manière que les autres personnes morales. Ces limitations sont essentielles, en particulier du point de vue des droits de l'homme, pour garantir que les responsables d'abus en répondent et protéger les victimes potentielles. Comme c'est le cas pour les sociétés, la responsabilité des personnes physiques derrière la personne morale pourrait être engagée en cas de comportements graves ou criminels.

Les difficultés relatives à la nature juridique des DAO sont parfaitement illustrées par ce qui est arrivé à *The DAO*, la première organisation de ce type, lancée en avril 2016. Dès ses premières semaines d'existence, *The DAO a* réussi à lever des sommes considérables, ce qui a immédiatement suscité l'attention. Le 17 juin 2016, un « attaquant » a exploité une faille dans la programmation qui lui a permis de s'approprier près de 55 millions de dollars US. Si l'acte commis semblait contraire à l'éthique et à l'objectif de la DAO, certains ont contesté que le détournement soit juridiquement répréhensible et puisse s'apparenter à un vol. En effet, la documentation de *The DAO* indiquait clairement que les conditions générales étaient définies par le code informatique du *smart contract* : or l'attaquant avait simplement exploité le code à son propre bénéfice.

L'attaque n'a pas donné lieu à une intervention judiciaire, mais à une solution décidée collectivement sur la plateforme Ethereum. L'ensemble de la communauté Ethereum, et pas seulement les membres de *The DAO*, a voté en faveur d'un « *hard fork* » consistant à modifier l'historique des transactions passées pour les supprimer de la blockchain, afin de revenir à l'état de la chaîne avant le détournement. Cette solution de réécriture des transactions était en contradiction directe avec le principe d'immutabilité de la blockchain, suscitant de vives critiques.

Si l'issue choisit a offert une solution aux détenteurs de jetons de *The DAO*, cette issue n'a pas apporté de réponse aux questions juridiques soulevées par l'affaire, qui dépassent la simple qualification juridique du comportement de l'« attaquant ». S'il n'avait pas été possible de revenir sur les écritures passées, les investisseurs de *The DAO* auraient-ils dû renoncer aux 50 millions de dollars détournés sans aucun recours ? Avaient-ils investi à leurs propres risques ou auraient-ils pu déposer une plainte contre les auteurs du code pour programmation défectueuse ? En outre, quelle pouvait être leur responsabilité envers des tiers à *The DAO* ? À supposer que *The DAO* puisse être considérée comme une société, tous les détenteurs de jetons devaient-ils être considérés comme également responsables ? Certains membres devaient-ils avoir d'une plus grande responsabilité, en fonction de leur rôle dans l'organisation ? Et comment identifier les détenteurs de jetons compte tenu de l'anonymat ? Cette affaire a montré la difficulté d'articuler l'apparition de ce nouveau type d'organisation en ligne avec les règles existantes.

Références

G'sell, Florence (2019), Intelligence artificielle et blockchain, in Bensamoun, Alexandra & Loiseau, Grégoire (2019), *Droit de l'intelligence artificielle*, Dalloz.

Martin-Bariteau, Florian & Marina Pavlović (2020), AI and Contract Law, in Florian Martin-Bariteau & Scassa, Teresa (éd.), *Artificial Intelligence and the Law in Canada*, LexisNexis.

Metjahic, Laila (2018), Deconstructing the DAO: The need for legal recognition and the application of securities laws to decentralized organizations, *Cardozo Law Review* 39 : 1533.

Reyes, Carla L., Nizan Geslevich Packin & Ben Edwards (2017), Distributed Governance, William & Mary Law Review Online 59 : 1.

Conclusion

Au fur et à mesure que la technologie blockchain se développe, ses applications permettant de résoudre des problèmes en lien avec le respect des droits de l'homme se multiplient. La blockchain peut être adaptée pour faire progresser la démocratie, assurer la responsabilité et la transparence, et garantir, par exemple, le respect des droits des réfugiés. Au cours des prochaines années, les acteurs du secteur, les États et le grand public devront se familiariser avec cette ressource inestimable et apprendre à l'utiliser pour accélérer les interventions humanitaires dans le monde entier. Il est dans l'intérêt du Conseil de l'Europe de se pencher sur la capacité de la technologie blockchain à appuyer sa mission de défense des droits de l'homme et de la démocratie sur le terrain. Cependant, comme nous l'avons montré, le déploiement de la blockchain s'accompagne d'un grand nombre de problèmes juridiques, dont des risques d'atteinte aux libertés et droits fondamentaux protégés par la Convention européenne des droits de l'homme et d'autres institutions internationales. Même si les crypto-anarchistes soutiennent le contraire, les registres distribués doivent être régulés afin de limiter les risques et les injustices.

Il semble essentiel que le Conseil de l'Europe déploie un programme de recherche et d'actions qui lui permette d'être pleinement conscient des avantages et des risques que présente la blockchain, et qu'il propose des instruments juridiques adaptés afin d'exploiter le potentiel de cette technologie tout en limitant ses possibles effets négatifs. Ce rapport n'a présenté qu'une vue d'ensemble ; plusieurs points particulièrement importants méritent d'être étudiés plus en détail.

En premier lieu, la technologie blockchain propose des solutions intéressantes pour le règlement des litiges et l'arbitrage, qui devraient être explorées plus avant. Il est par ailleurs nécessaire de s'assurer que les solutions proposées sur la blockchain garantissent le respect des droits procéduraux, en particulier le droit à un procès équitable.

En deuxième lieu, les identités décentralisées et les solutions de gouvernance des données ont le potentiel de redonner aux utilisateurs le contrôle de leurs données et de mieux protéger leur vie privée. Des réglementations adaptées sont cependant nécessaires pour s'assurer que ces solutions garantissent effectivement les droits des utilisateurs sur leurs données et ne reviennent pas à monnayer leurs informations personnelles. Par conséquent, ces solutions devraient être étudiées plus avant par le Conseil.

En troisième lieu, il est indispensable que le Conseil réfléchisse à l'articulation complexe entre le chiffrement et les libertés fondamentales. Cette réflexion est particulièrement nécessaire à l'heure où certains États démocratiques envisagent d'interdire le chiffrement pour des raisons liées à la lutte contre le terrorisme et les activités illicites. Si le chiffrement peut dissimuler certaines activités illicites, il permet également de protéger notre vie privée, nos institutions et nos libertés fondamentales, notamment la liberté d'expression et la liberté de la presse. Un juste équilibre doit être trouvé entre le respect des libertés et la nécessité pour les États d'assurer l'ordre public.

Enfin, le Conseil de l'Europe pourrait s'attaquer à plusieurs problèmes qui ont un impact sur les droits fondamentaux des individus et doivent être résolus. Le Conseil pourrait par exemple proposer des principes et des instruments pour régler le problème de la détermination du droit applicable et des juridictions compétentes pour les registres distribués. Le Conseil pourrait aussi fournir des orientations sur la mesure dans laquelle l'automatisation est acceptable du point de vue des droits fondamentaux.

Dans l'ensemble, le Conseil de l'Europe devrait continuer à soutenir les recherches et les discussions relatives à l'impact de la blockchain sur les droits de l'homme, la démocratie et l'État de droit. À l'image des initiatives réussies du Conseil en matière d'intelligence artificielle, il serait intéressant de lancer des travaux pluripartites sur la blockchain et les registres distribués. Cela permettrait de promouvoir de bonnes pratiques et de proposer des lignes directrices et des recommandations — voire de préconiser de nouveaux instruments juridiques pour promouvoir le développement responsable de cette technologie.

Annexe — Blockchain et Convention européenne des droits de l'homme

Droits fondamentaux	Avantages	Risques
Droit à la liberté et à la sûreté (article 5)	➔ Le pseudo-anonymat sur la blockchain garantit la liberté et la confidentialité. ➔ Les techniques d'identification fournies par la blockchain favorisent l'autonomie des citoyens. ➔ Les techniques d'identification fournies par la blockchain permettront aux personnes vulnérables de s'identifier de manière sécurisée pour faire valoir leurs droits et accéder aux services essentiels (alimentation, santé, éducation, etc.).	➔ Le pseudo-anonymat ne rend pas entièrement impossible l'identification des individus qui interagissent sur la blockchain. ➔ L'automatisation grâce aux *smart contracts* rend leurs utilisateurs prisonniers d'un programme informatique.
Droit à un procès équitable (article 6)	➔ Les modes de règlement des litiges proposés sur la blockchain sont confidentiels, rapides et efficaces.	➔ Il est difficile de déterminer de quelles juridictions et de quel droit relèvent les transactions sur des blockchains publiques. ➔ Les modes alternatifs de règlement des litiges proposés sur la blockchain pourraient ne pas respecter les droits procéduraux les plus essentiels. ➔ Le pseudo-anonymat des utilisateurs et l'incertitude quant à la nature juridique des DAO constituent des obstacles à la garantie des droits des détenteurs de jetons.

Droits fondamentaux	Avantages	Risques
Droit au respect de la vie privée et familiale (article 8)	➔ Le pseudo-anonymat sur la blockchain protège la vie privée et les données personnelles. ➔ Les plateformes entièrement chiffrées (plateformes de *privacy coins*) et les blockchains qui prévoient la confidentialité par défaut garantissent un quasi-anonymat, dans le respect du droit à la vie privée.	➔ Sur de nombreuses blockchains, le pseudonymat est relatif, car la réidentification n'est pas impossible et les utilisateurs sont généralement obligés de divulguer leur identité lorsqu'ils créent leur portefeuille numérique.
Liberté d'expression (article 10)	➔ Le pseudo-anonymat sur la blockchain est une garantie du droit à la liberté d'expression.	➔ Le pseudo-anonymat sur la blockchain peut être levé, surtout pour les utilisateurs qui ont créé leur portefeuille numérique chez des prestataires qui appliquent une procédure de connaissance de la clientèle (KYC).
Liberté de réunion pacifique et d'association (article 11)	➔ la coopération de multiples utilisateurs sur la blockchain constitue, au sens le plus large, une forme d'exercice de la liberté d'association.	

Droits fondamentaux	Avantages	Risques
Droit à la protection de la propriété (Protocole n° 1, article 1)	➔ Les NFT peuvent faciliter la gestion et l'immatriculation de biens numériques. ➔ Dans le domaine de l'immobilier, les *smart contracts* peuvent faciliter la gestion des baux et des titres. ➔ Là où les systèmes de gestion de la propriété foncière sont défaillants, la blockchain peut permettre d'établir des registres de propriété foncière fiables et de prévenir la fraude.	➔ Les attaques et failles de sécurité, comme lors de l'affaire *The DAO*, peuvent entraîner des détournements et des pertes de biens.
Droit de participer à des élections libres (Protocole n° 1, article 3)	➔ La blockchain permet de déployer des systèmes de vote en ligne fiables : les électeurs déposent leur bulletin de vote chiffré sur une blockchain en accès public et peuvent s'assurer que leur voix a été correctement enregistrée. On peut aussi imaginer que la plateforme ne soit pas gérée par l'État seul, mais par différentes parties prenantes (municipalités, régions, partis politiques, organisations de la société civile, etc.).	

Droits fondamentaux	Avantages	Risques
Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108)	➔ Les plateformes entièrement chiffrées et les blockchains prévoyant par défaut la confidentialité des données garantissent que les utilisateurs ne sont pas identifiables. ➔ Les récentes méthodes de stockage hors chaîne des données, qui rendent les données consultables uniquement après validation par l'utilisateur, peuvent être un moyen très sûr de donner le contrôle à l'utilisateur et de partager des données sensibles dans le respect de la législation encadrant la protection des données.	➔ Sur la blockchain, le pseudo-anonymat est relatif, car la réidentification n'est pas impossible et les utilisateurs sont généralement obligés de divulguer leur identité lorsqu'ils créent leur portefeuille numérique. ➔ L'immutabilité de la blockchain ne permet pas de supprimer des données personnelles sensibles, ce qui entre en contradiction avec le droit à la suppression et à la modification des données.
Droit à un environnement sain (Résolution du Parlement du Conseil de l'Europe, *Combattre les inégalités dans le droit à un environnement sûr, sain et propre*, septembre 2021 ; ainsi que articles 2 [droit à la vie], 5 [liberté et sécurité] et 8 [respect de la vie privée et familiale] tels qu'interprétés par la Cour européenne des droits de l'homme).		➔ La consommation énergétique de la blockchain et en particulier de certains protocoles techniques (comme la preuve de travail) entraîne un bilan environnemental problématique.

Le présent rapport étudie les avantages et les risques potentiels de la technologie blockchain pour la démocratie, les droits de l'homme et l'État de droit.

À partir de l'étude de plusieurs exemples d'applications fondées sur la blockchain, ce rapport formule, à l'intention du Conseil de l'Europe, une première série de recommandations relatives aux recherches devant être menées dans ce domaine à l'avenir et aux axes de réflexion devant être privilégiés.

Le rapport met en évidence les caractéristiques les plus prometteuses de la blockchain et de ses applications, telles les crypto-monnaies, les smart contracts, les organisations autonomes décentralisées (DAO) ou les jetons non fongibles (NFT).

L'étude présente aussi les limites de la technologie, qui sont non négligeables et font peser un risque d'atteinte aux droits fondamentaux.

www.coe.int

Le **Conseil de l'Europe** est la principale organisation de défense des droits de l'homme du continent. Il comprend 46 États membres, dont l'ensemble des membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits de l'homme, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres du Conseil de l'Europe.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE