Nations Unies A/CN.9/1175

Assemblée générale

Distr. générale
29 mai 2024
Français
Original : anglais

Commission des Nations Unies pour le droit commercial international
Cinquante-septième session
New York, 24 juin-12 juillet 2024

Questions juridiques liées à l'utilisation de la technologie des registres distribués dans le commerce

Note du Secrétariat

Table des matières

V.24-09233 (F) 050724 080724

I. Informations générales

1. Consciente du fait que la CNUDCI jouait un rôle central et de coordination au sein du système des Nations Unies dans le traitement des questions juridiques liées à l'économie et au commerce numériques (A/74/17, par. 211), à sa cinquante-cinquième session, en 2022, la Commission a prié le secrétariat d'élaborer un document d'orientation sur les questions juridiques liées à l'utilisation de systèmes de registres distribués dans le commerce, dans la limite des ressources existantes et en coopération avec d'autres organisations concernées, le cas échéant (A/77/17, par. 22 f) et 169). Elle a formulé cette requête dans le cadre de l'élaboration d'une section de la *Taxonomie des questions juridiques liées à l'économie numérique* (la « Taxonomie ») consacrée aux systèmes de registres distribués.

2. À sa cinquante-sixième session, en 2023, la Commission était saisie d'une note du secrétariat sur les questions juridiques liées à l'utilisation de la technologie des registres distribués dans le commerce (le « document de cadrage ») (A/CN.9/1146). Elle a pris note avec satisfaction du contenu de ce document et a souligné sa transversalité dans le contexte d'autres chantiers de la CNUDCI sur le commerce numérique, notamment les travaux menés par les Groupes de travail II, IV et V. On a largement appuyé l'idée de mener les travaux en étroite coordination avec d'autres organisations internationales concernées, et on a noté que ces travaux seraient pertinents pour plusieurs projets récemment entrepris par la Conférence de La Haye de droit international privé (« HCCH ») (A/78/17, par. 200 à 202).

3. En conséquence, la Commission a demandé au secrétariat de poursuivre et de mener à bien les travaux en vue d'élaborer un document d'orientation sur les questions juridiques liées à l'utilisation des systèmes de registres distribués dans le commerce, dans la limite des ressources existantes et en coopération avec d'autres organisations concernées, selon qu'il conviendrait [A/78/17, par. 22 c)].

4. La présente note s'appuie sur le document de cadrage et le complète en apportant un éclairage supplémentaire sur les questions juridiques liées à l'utilisation de la technologie des registres distribués dans le commerce. Elle ne se prononce pas sur la question de savoir si celle-ci est appropriée pour l'utilisation envisagée. Elle indique les domaines dans lesquels on trouvera des orientations juridiques et propose des solutions pouvant s'inscrire dans le cadre des instruments juridiques existants. Elle recense également les domaines dans lesquels il n'existe pas encore de solution juridique établie en raison de la nouveauté de la technologie des registres distribués et présente alors dans les grandes lignes ces situations en pleine évolution. Le secrétariat compte l'étoffer, notamment avec l'aide d'experts, et y inclure, en coopération avec les organisations concernées, des informations sur des questions complémentaires telles que l'interaction entre cette technologie et les accords de libre-échange. En particulier, la HCCH a pour mandat de collaborer avec la CNUDCI et d'autres organisations disposant d'une expertise pertinente sur les aspects de droit international privé de l'économie numérique[1]. Les résultats de ses travaux devraient pouvoir être utilement intégrés dans le document d'orientation.

5. La présente note contient en annexe un glossaire des termes techniques. La première occurrence de chaque terme défini figure en italique. Le glossaire pourra être enrichi au fur et à mesure de l'avancement des travaux sur le document d'orientation.

[1] Conclusions et décisions du Conseil sur les affaires générales et la politique (CAGP) (C&D de mars 2024), n° 11 b), disponibles sur le site Web de la HCCH, à l'adresse www.hcch.net, sous « Gouvernance » puis « Conseil sur les affaires générales et la politique ».

II. Contenu du document d'orientation

A. Informations générales sur la technologie des registres distribués

6. La Taxonomie contient la définition pratique suivante de la technologie des registres distribués : « ensemble de technologies et de méthodes qui sont déployées pour mettre en œuvre et tenir un registre (ou base de données) qui est partagé, répliqué et synchronisé sur plusieurs ordinateurs (ou serveurs) mis en réseau. Le système de registre distribué est donc le système (composé d'éléments logiciels et matériels) qui permet le déploiement de ces technologies et méthodes. Ces systèmes diffèrent en termes de conception, de gouvernance, d'objectif et d'utilisation » (Taxonomie, par. 172).

7. Selon une autre définition, la technologie des registres distribués correspond à une base de données décentralisée sur un réseau pair à pair de machines, généralement reliées par Internet. Elle peut être conçue de façon à permettre à plusieurs parties d'enregistrer et de mettre à jour des informations. Cette technologie met généralement en œuvre plusieurs éléments tels qu'une infrastructure informatique, une connexion Internet et des données. D'un point de vue technique, ces éléments comprennent généralement un *hachage cryptographique* (des données d'un bloc, par exemple), un *mécanisme de consensus* (par exemple, *preuve par l'enjeu*), une plateforme (telle qu'un protocole de la couche 1) et des actifs numériques (par exemple, des jetons fongibles).

8. La technologie de la chaîne de blocs est une forme largement connue de technologie des registres distribués. Elle permet d'archiver des données au moyen d'une chaîne de blocs. Chaque bloc contient des données, telles qu'un registre des transactions, et un résumé – souvent un hachage cryptographique – formant un lien avec le bloc précédent. Toute modification d'une transaction dans un bloc antérieur induit une modification du hachage du bloc associé, ce qui se répercute ensuite sur les hachages de tous les blocs consécutifs. Ainsi, pour modifier des informations sur la chaîne de blocs, il faut modifier chaque bloc suivant dans l'ordre chronologique, puis diffuser sur le réseau le registre numérique mis à jour, avant l'ajout d'un nouveau bloc au registre par une autre entité. En réalité, cette procédure ne peut pas être mise en œuvre dans des réseaux passablement développés. L'enregistrement de la transaction est donc persistant. Cette caractéristique est également appelée « immuabilité ».

B. Classification des systèmes de registres distribués

9. Les systèmes de registres distribués peuvent être classés selon deux caractéristiques essentielles, à savoir selon que le registre est public ou privé et selon qu'il est accessible avec ou sans permission (Taxonomie, par. 178). Cette classification a été établie à titre d'exemple et n'est pas représentative de la grande variété de solutions disponibles.

10. La nature publique ou privée des registres distribués est déterminée par la question de savoir qui peut participer au développement du système de registre distribué en tant qu'*opérateur de nœud*, c'est-à-dire en tant qu'opérateur d'un ordinateur faisant partie du réseau du registre. L'expression « registre public » se rapporte à un système décentralisé offrant un accès libre. À l'inverse, l'accès à un « registre privé » est limité à un groupe restreint de participants prédéterminés.

11. On parle de registres distribués avec ou sans permission selon qu'il est nécessaire ou non d'obtenir une permission pour y participer, c'est-à-dire que l'identification de l'utilisateur est une condition préalable à la participation. Dans un registre sans permission, aucune identification n'est requise : en théorie, tout utilisateur peut participer au registre sans avoir à s'identifier. Dans un registre avec permission, les utilisateurs doivent s'identifier avant de pouvoir accéder au registre,

et des mesures sont généralement mises en place pour permettre la gestion de l'identité.

12. Un registre distribué public sans permission est l'option la plus ouverte et la plus décentralisée. Tout un chacun peut y participer sans vérification d'identité et il n'y a généralement pas d'administrateurs chargés de restreindre la possibilité pour les utilisateurs ou les participants d'y accéder, de le consulter et d'y enregistrer des données[2].

13. L'un des principaux avantages d'un registre distribué public sans permission est sa conception transparente, qui favorise l'évolutivité puisque les nouveaux acteurs n'ont pas besoin de se soumettre au contrôle d'une entité directrice. Tout acteur peut accéder et contribuer à ce registre sans permission ou autorisation préalable, à condition de respecter la gouvernance autorégulée du réseau.

14. Les principales caractéristiques des registres distribués publics sans permission sont les suivantes :

a) Libre accès : le réseau n'est pas contrôlé par un administrateur unique, ce qui limite efficacement la possibilité d'influence d'un acteur unique ;

b) Source ouverte : le code source est accessible au public et n'importe qui peut proposer des modifications ;

c) Transparence : toutes les données du registre distribué sont visibles publiquement, bien que le *pseudonymat* et d'autres dispositifs permettent un certain degré de confidentialité ;

d) Sécurité : l'utilisation de techniques cryptographiques garantit l'intégrité du réseau en s'appuyant sur la confiance dans le système plutôt que sur la confiance dans une seule entité centrale de contrôle. Cette approche est dite « sans confiance » car elle ne nécessite aucune source de confiance externe ;

e) Pseudonymat : les acteurs sont identifiés par des pseudonymes au niveau de l'infrastructure.

15. À l'inverse, un registre privé avec permission limite le nombre d'utilisateurs et de participants et exige l'identification préalable de ces participants. Ce type de registre est normalement créé par les entreprises et utilisé au sein de celles-ci. Il est fortement réglementé et contrôlé par l'entreprise qui l'a créé et qui l'exploite.

16. Les principales caractéristiques des registres distribués privés avec permission sont les suivantes :

a) Accès restreint : seuls les acteurs autorisés peuvent accéder et participer au registre ;

b) Source fermée : le code n'est souvent pas accessible au public sous la forme utilisée pour le registre ;

c) Contrôle : une entité (organisation ou groupe) contrôle le registre, de sorte que seuls certains acteurs peuvent y accéder ;

d) Confidentialité : l'accès restreint au registre permet de mieux protéger les données à des fins de respect de la vie privée et de confidentialité ;

e) Vitesse de transaction accrue : le niveau de confiance entre les acteurs étant plus élevé, le protocole de consensus peut permettre davantage de transactions par unité de temps.

17. On trouve aussi, bien que rarement, des registres publics avec permission et des registres privés sans permission. Un registre public avec permission exige l'identification préalable des participants, mais n'impose pas de restrictions quant aux personnes qui peuvent participer. Un registre privé sans permission fixe des

[2] Le Bitcoin et l'Ethereum sont des exemples de registres distribués publics sans permission. Le registre du Bitcoin contient l'historique de chaque transaction en bitcoins, accessible à tous.

restrictions en ce qui concerne les participants, mais n'exige pas d'eux qu'ils s'identifient.

C. Caractéristiques associées à l'utilisation de la technologie des registres distribués

Persistance de l'information

18. La persistance de l'information (ou « immuabilité ») est une caractéristique essentielle de la technologie des registres distribués. Un consensus est nécessaire pour modifier l'information stockée dans le registre, ce qui permet de mieux garantir l'intégrité de cette information, notamment contre les modifications unilatérales (voir par. 8 ci-dessus). D'une manière générale, il importe que les entreprises qui utilisent la technologie des registres distribués dans leurs opérations envisagent soigneusement les implications de l'immuabilité, et qu'elles mettent en place des mesures appropriées pour résoudre les problèmes qui pourraient survenir.

19. La persistance de l'information peut avoir des conséquences considérables. Par exemple, si tous les actifs d'une entreprise sont correctement enregistrés dans des registres distribués, il peut être plus facile d'en déterminer l'existence (mais pas nécessairement d'en évaluer la valeur), y compris dans des cas particuliers comme lorsqu'une restructuration préalable à l'insolvabilité est envisagée.

20. Compte tenu de la persistance de l'information, il est important de veiller à l'exactitude des données stockées dans le registre distribué. Les entreprises peuvent envisager de mettre en place des systèmes susceptibles de prévenir la saisie incorrecte de données, consistant par exemple à diffuser au sein du réseau les données à saisir dans le registre, ou à établir des lignes directrices internes sur la confirmation de l'exactitude des données et les restrictions concernant leur saisie.

21. En fonction de la gouvernance et du type de système de registre distribué, il existe un risque que des failles soient exploitées aux fins de modification des informations contenues dans le registre. Par exemple, dans un registre distribué qui utilise la *preuve de travail*, un groupe de validateurs contrôlant plus de 50 % du *taux de hachage de minage* du réseau peut modifier le registre numérique. Toutefois, lorsqu'un registre distribué atteint une certaine taille, l'obligation de contrôler plus de 50 % de ce taux entraîne des coûts prohibitifs[3] et a peu de chances d'être remplie par quiconque voudrait mener à son terme un acte malveillant.

22. Il peut arriver que l'entité gérant le registre distribué décide d'apporter au protocole des modifications incompatibles avec les blocs antérieurs. Cela peut également compromettre la persistance de l'information.

Caractère définitif des transactions

23. Les transactions effectuées à l'aide de la technologie des registres distribués sont diffusées et réparties au sein du réseau. En général, on considère une transaction comme définitive lorsqu'elle est irréversible et qu'un bloc a été ajouté au registre et ne peut pas être supprimé. Il s'ensuit que dans certains systèmes de registres distribués, la transaction ne devient définitive que lorsque le réseau est convenu d'accepter le bloc[4]. Celle-ci est alors considérée comme irrévocable et son inscription au registre acquiert un caractère définitif.

---

[3] Il s'agit du coût à supporter pour contrôler 51 % du registre distribué en achetant la cryptomonnaie nécessaire au taux de capitalisation boursière.

[4] Par exemple, dans le cas du bitcoin, une transaction devient définitive dès lors qu'environ six nouveaux blocs sont ajoutés au registre numérique après le bloc qui la contient.

Exécution automatisée non discrétionnaire

24. Une autre caractéristique de la technologie des registres distribués est la nature moindrement discrétionnaire de l'exécution des commandes que contiennent les scripts stockés dans le registre distribué (contrats automatisés basés sur la technologie des registres distribués ou « contrats intelligents »). Comme d'autres contrats automatisés, un contrat automatisé basé sur cette technologie s'exécute automatiquement lorsque des conditions prédéfinies sont remplies. Les parties n'ayant pas la possibilité de modifier unilatéralement les scripts, la certitude que les instructions seront exécutées est plus grande, ce qui améliore l'efficacité et la prévisibilité des opérations. Toutefois, cet aspect peut poser problème lorsque la loi exige l'inclusion d'un logiciel qui arrête l'exécution de la clause automatisée (*bouton d'arrêt d'urgence* ou « *kill switch* »)[5].

Pseudonymat

25. L'utilisation de pseudonymes n'empêche pas nécessairement l'identification de la partie, mais elle peut la rendre difficile, en particulier si la loi exige l'utilisation d'une méthode ou procédure particulière, ou exige un certain niveau de garantie pour l'identité. Si l'identification fiable n'est pas possible, des mesures supplémentaires telles que la détection des anomalies et des fraudes[6] peuvent être nécessaires, par exemple pour éviter que les actifs numériques stockés dans le registre ne fassent l'objet d'opérations d'initiés.

26. Une partie utilisant un pseudonyme peut être identifiée grâce à des éléments factuels. Par exemple, s'agissant de l'exigence d'identification énoncée à l'article 9 de la Loi type de la CNUDCI sur les documents transférables électroniques (« LTDTE ») en ce qui concerne les signatures électroniques utilisées dans les documents transférables électroniques, « [l']identification, avec la possibilité d'associer pseudonyme et nom véritable, notamment à partir d'éléments factuels extérieurs au système de registre distribué, peut satisfaire à l'exigence d'identification du signataire » (note explicative relative à la LTDTE, par. 78).

27. Un problème particulier peut se poser lors de l'envoi de notifications légales à une adresse pseudonyme. Dans les pays où le droit est plus souple sur ces questions, des procédures spécifiques ont été mises au point pour la signification d'actes judiciaires, notamment dans les affaires relatives aux cryptomonnaies. Par exemple, des tribunaux ont tenté de signifier de tels actes en passant par les médias sociaux ou en délivrant un message à l'adresse du portefeuille de cryptomonnaies du défendeur. Certains ont également autorisé la signification d'actes au moyen de *jetons non fongibles* distribués dans le portefeuille (« largage »)[7]. Toutefois, dans certains pays,

---

[5] Voir, par exemple, l'article 36-1 b), du Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données), JO L, 2023/2854, 22.12.2023, ELI : http://data.europa.eu/eli/reg/2023/2854/oj, qui exige (notamment) que les contrats automatisés basés sur la technologie des registres distribués respectent l'une des exigences essentielles relatives à la résiliation et à l'interruption en toute sécurité, à savoir « veiller à ce qu'il existe un mécanisme permettant de mettre fin à l'exécution continue des transactions et à ce que le contrat intelligent intègre des fonctions internes qui peuvent réinitialiser le contrat ou lui donner instruction de cesser ou d'interrompre l'opération, en particulier pour éviter de futures exécutions accidentelles ».

[6] Les mécanismes de détection consistent notamment à analyser les données (soit statistiquement, soit à l'aide de l'apprentissage automatique) pour détecter toute anomalie dans les activités et les schémas.

[7] *LCX Ag* c. *1.274M U.S. Dollar Coin*, nº 154644/2022, 2022 WL 3585277 (N.Y. Sup. Ct., 21 août 2022) ; *Jones* c. *X* [2022] EWCH 2543 (Comm) ; *Benjamin Arthur Bowe*n c. *Xingzhao Li* (affaire nº 23-cv-20399) (S.D. Fla. 2023, 3 mars 2023).

le recours à ces mécanismes est considéré comme une violation des garanties de procédure[8].

Manque d'interopérabilité

28. En général, l'interopérabilité entre registres est insuffisante dans la technologie des registres distribués, c'est-à-dire qu'un registre distribué n'est pas conçu pour interagir avec un autre ou avec des applications n'utilisant pas cette technologie. En effet, les registres distribués, en particulier ceux qui sont privés et adaptés à des besoins particuliers, sont conçus en fonction d'un ou de plusieurs objectifs précis et ne fonctionnent pas en dehors de ce cadre. Le manque d'interopérabilité peut limiter leurs applications et leurs avantages, car les informations restent cantonnées dans un « *silo de données* » et ne peuvent pas être facilement transmises ou utilisées dans d'autres systèmes. Des travaux techniques ont été entrepris pour dépasser cette limite technique[9] et parvenir à une normalisation propice à l'interopérabilité[10].

D. Droit applicable à la technologie des registres distribués

Principes sous-tendant les textes de la CNUDCI sur le commerce électronique

Neutralité technologique

29. Le principe de neutralité technologique est un élément essentiel des textes de la CNUDCI sur le commerce électronique. Il exige l'adoption de dispositions juridiques neutres quant aux technologies, méthodes et produits utilisés. Cela signifie qu'en cas d'avancées technologiques, il n'est pas nécessaire d'entreprendre de nouveaux travaux législatifs, car des règles neutres sur le plan technologique tiennent déjà compte de toute évolution future. La neutralité technologique fait que les textes de la CNUDCI sont généralement favorables à l'utilisation de la technologie des registres distribués.

30. La définition du « document électronique » énoncée à l'article 2 de la LTDTE a été étendue pour englober « toute l'information logiquement associée ou autrement jointe au document de façon à en devenir partie, qu'elle soit créée simultanément ou non », afin de confirmer qu'elle s'applique aux applications basées sur la technologie des registres distribués. Cette définition est étroitement liée à celle du « message de données », qui garantit la neutralité technologique des textes de la CNUDCI sur le commerce électronique.

Reconnaissance juridique

31. Les dispositions contenues dans les textes de la CNUDCI accordent une reconnaissance juridique à l'utilisation de moyens électroniques (et interdisent toute discrimination à l'égard de cette utilisation) sur une base technologiquement neutre. Elles s'appliquent donc également à l'utilisation de la technologie des registres distribués.

32. Par contre, comme la technologie des registres distribués repose sur l'utilisation de techniques de chiffrement, les pays qui ont adopté des lois limitant le recours à ces techniques (par exemple, en conférant uniquement des effets juridiques aux signatures électroniques émises conformément aux normes et systèmes nationaux de chiffrement) peuvent restreindre la capacité à accorder une reconnaissance juridique à l'utilisation de cette technologie. En outre, ce choix législatif peut être incompatible avec les dispositions des accords commerciaux qui imposent l'utilisation de méthodes

[8] *X* c. *Y*, Gerechtshof Amsterdam, 29 janvier 2019, ECLI:NL:GHAMS:2019:192, décision 1921 du Recueil de jurisprudence.

[9] Voir, par exemple, le protocole interchaînes de Chainlink et l'écosystème du réseau Polkadot.

[10] Voir, par exemple, le programme technique du comité technique ISO/TC307 sur les technologies des chaînes de blocs et les technologies de registre distribué.

de signature électronique ou d'authentification électronique technologiquement neutres.

Équivalence fonctionnelle

33. Le principe d'équivalence fonctionnelle permet de satisfaire aux exigences de forme applicables aux documents papier en utilisant des moyens électroniques. Outre le respect de certaines conditions, il suppose l'emploi de méthodes fiables pour atteindre l'objectif visé. Les caractéristiques de la technologie des registres distribués, telles que la persistance de l'information et la garantie de la singularité, peuvent aider à remplir certaines exigences en matière d'équivalence fonctionnelle énoncées dans les textes de la CNUDCI.

34. Comme indiqué précédemment (Taxonomie, par. 200), les technologies et méthodes utilisées par un système de registre distribué pour mettre en œuvre ce registre rendent les données qui y sont enregistrées « immuables », c'est-à-dire qu'elles restent complètes et inchangées à partir du moment où elles ont été saisies dans le registre. Ces qualités correspondent au concept d'« intégrité » visé dans les textes de la CNUDCI sur le commerce électronique, qui est pertinent pour certaines règles d'équivalence fonctionnelle :

a) L'article 8 de la Loi type de la CNUDCI sur le commerce électronique (« LTCE ») considère que l'intégrité est l'une des fonctions qu'un message de données contenant des informations doit remplir afin de satisfaire à l'exigence légale tendant à ce qu'une information soit présentée ou conservée sous sa forme originale. Cette fonction est remplie si l'information est restée « complète » et n'a « pas été altérée » à compter du moment où elle a été créée pour la première fois sous sa forme définitive, exception faite de l'ajout de tout endossement et de toute modification intervenant dans le cours normal de la communication, de la conservation et de l'exposition. La même exigence figure à l'article 9-4 de la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux (« CCE »). Les méthodes qui utilisent la technologie des registres distribués peuvent offrir un niveau de fiabilité plus élevé en ce qui concerne la garantie de l'intégrité ;

b) En vertu de l'article 10 de la LTDTE, l'intégrité est l'une des fonctions qu'un document transférable électronique doit remplir pour être juridiquement équivalent à un document ou à un instrument transférable papier ;

c) L'article 6-3 d) de la Loi type de la CNUDCI sur les signatures électroniques (« LTSE ») reconnaît que certains types de signatures électroniques permettent de déceler toute modification apportée à l'information signée. Cette fonction est généralement remplie par les signatures électroniques qui utilisent des techniques cryptographiques et peut donc se trouver également dans les systèmes de registres distribués. Dans le même ordre d'idées, l'article 17 de la Loi type de la CNUDCI sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance (« LTIC ») prévoit l'intégrité comme l'une des fonctions des cachets électroniques.

35. De même, la persistance de l'information peut aider à satisfaire aux exigences en matière de preuve énoncées dans les textes de la CNUDCI. Par exemple :

a) L'article 9 de la LTCE indique que la force probante d'un message de données s'apprécie eu égard, entre autres, à la fiabilité du mode de préservation de l'intégrité de l'information ;

b) L'article 19 de la LTIC, relatif aux services d'archivage électronique, exige que le message de données archivé soit conservé dans le format sous lequel il a été créé, transmis ou reçu, ou dans un autre format dont il peut être démontré qu'il permet de détecter toute altération du message après cette date et cette heure, exception faite de l'ajout de toute modification intervenant dans le cours normal de la communication, du stockage et de l'affichage.

36. À cet égard, en droit de l'Union européenne (« UE »)[11], l'utilisation d'un service de confiance appelé « registre électronique » est associée à une présomption quant au classement chronologique séquentiel unique et précis et à l'intégrité des enregistrements de données qu'il contient lorsque certaines conditions supplémentaires sont remplies (« registre électronique qualifié »). Dans la même loi, le « registre électronique » est défini comme « une séquence d'enregistrements de données électroniques qui garantit l'intégrité de ces enregistrements et l'exactitude du classement chronologique de ces enregistrements »[12].

37. La singularité est l'assurance que l'objet numérique (par exemple un document commercial sous forme électronique) n'existe que dans un unique enregistrement électronique. Les jetons non fongibles sont une application particulière de la technologie des registres distribués dont les caractéristiques techniques permettent de mieux garantir la singularité d'un objet numérique. Ainsi, par exemple, ils peuvent faciliter le respect de l'exigence de singularité des documents transférables électroniques énoncée à l'article 10-1 b) i) de la LTDTE.

Utilisation de la technologie des registres distribués dans le cadre de la contractualisation électronique

Emplacement du matériel

38. La technologie des registres distribués étant de nature décentralisée, ses différents éléments peuvent se trouver dans des pays différents, ou peuvent également changer régulièrement d'emplacement. C'est pourquoi les règles indiquant que l'endroit où se trouvent le matériel et la technologie sur lesquels s'appuie un système d'information ne constitue pas nécessairement l'établissement d'une partie (art. 6-4 de la CCE) peuvent être utiles en cas de recours à la technologie des registres distribués. La définition d'un « système d'information » comme « un système utilisé pour créer, […] recevoir, conserver ou traiter de toute autre manière des messages de données » (art. 2 f) de la LTCE et art. 4 f) de la CCE) englobe les registres distribués.

Exécution automatisée

39. Comme on l'a noté plus haut (par. 24), l'utilisation de la technologie des registres distribués peut renforcer la confiance dans l'exécution automatisée des contrats en réduisant la possibilité de les modifier unilatéralement. Les contrats automatisés basés sur cette technologie peuvent être configurés de façon à s'exécuter automatiquement lorsque certains paramètres sont remplis. Les métadonnées et les données créées par des objets hors registre tels que les oracles peuvent également conditionner le déclenchement de l'exécution automatisée des contrats[13].

40. D'un point de vue pratique, il convient de noter que l'exécution automatisée des clauses contractuelles peut s'avérer difficile lorsque celles-ci, telles la clause de force majeure et la clause compensatoire, nécessitent la prise en compte de faits et de circonstances spécifiques. On peut soutenir qu'il est possible d'établir et de préciser ces faits et circonstances aux fins de l'exécution automatisée. Toutefois, eu égard au nombre de conditions à clarifier et à la complexité des scénarios, les parties contractantes peuvent juger plus pratique de ne pas automatiser ces clauses.

---

[11] Article 45 *duodecies* du Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (« Règlement eIDAS »), tel que modifié par le Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le Règlement (UE) nº 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique (« Règlement eIDAS 2 »).

[12] Article 3-52 du Règlement eIDAS, tel que modifié.

[13] L'exécution d'un contrat automatisé basé sur la technologie des registres distribués pourrait par exemple être déclenchée en présence de certains paramètres, tels que la géolocalisation d'un navire ou l'échéance d'un paiement.

Signatures électroniques

41. D'un point de vue technique, la cryptographie est au cœur de la technologie des registres distribués. Les signatures électroniques reposant sur cette technique sont utilisées dans les registres distribués pour authentifier et autoriser les opérations exécutées dans le cadre de contrats automatisés.

42. Sur le plan juridique, les signatures électroniques basées sur la technologie des registres distribués peuvent servir à identifier le signataire et à exprimer son intention concernant le message signé, satisfaisant ainsi aux conditions de l'équivalence fonctionnelle entre signatures électroniques et manuscrites prévues dans les textes de la CNUDCI. Réciproquement, les principes de neutralité technologique et de non-discrimination à l'égard de l'utilisation de moyens électroniques qui sous-tendent ces textes s'appliquent également aux signatures électroniques utilisant la technologie des registres distribués, qui pourraient donc être légalement reconnues.

43. D'un autre côté, la loi peut exiger l'utilisation de technologies ou de services spécifiques (comme les « signatures qualifiées » ou les « signatures numériques ») et imposer l'utilisation de normes techniques internes et de fournisseurs nationaux (voir par. 32 ci-dessus). Les signatures électroniques basées sur la technologie des registres distribués peuvent ne pas répondre à ces exigences supplémentaires, par exemple parce que leur nature décentralisée ne permet pas de circonscrire à un pays unique le système de registre distribué.

44. Une application particulière des signatures électroniques dans l'environnement des registres distribués consiste dans l'utilisation de *portefeuilles multisignatures (« multisig »)*, notamment aux fins d'approbation de transactions portant sur des actifs numériques. Dans ce cas de figure, plusieurs signatures fondées sur l'infrastructure à clefs publiques (ICP) et provenant d'adresses prédéfinies sont nécessaires pour procéder à la transaction. Plus généralement, cette technologie peut être utilisée lorsque plusieurs signatures apposées par différentes parties sont requises pour autoriser une transaction (par exemple, dans la passation de marchés publics, pour les comptes de garantie bloqués, etc.).

Technologie des registres distribués et droit international privé

45. Des problèmes peuvent se poser sur le plan du droit international privé en raison de la multiplicité des pays susceptibles de jouer un rôle dans le fonctionnement et l'utilisation de la technologie des registres distribués, et de la difficulté de s'entendre sur le choix de la loi applicable, en particulier dans le cas des registres sans permission.

46. En général, les règles de droit international privé aident à déterminer la loi applicable. Toutefois, dans la couche « infrastructure » (voir par. 47 ci-dessous), les acteurs d'un système de registre distribué peuvent être dispersés dans plusieurs pays, et le registre lui-même peut se trouver dans plusieurs pays, ou son emplacement peut varier constamment. C'est pourquoi les règles de droit international privé qui se réfèrent à des éléments de rattachement territorial ne se prêtent pas nécessairement au contexte de la technologie des registres distribués[14].

[14] Voir HCCH, Doc. prél. nº 4 de novembre 2020, annexe I, pour une liste des éléments de rattachement de droit international privé et leur utilisation dans le contexte de la technologie des registres distribués.

E. Questions relatives à la couche « infrastructure »

47. La couche « infrastructure » des systèmes de registres distribués correspond au réseau et au registre distribué qui l'utilise. Le matériel, les données, le consensus et la programmation en sont les composantes importantes. Les acteurs concernés sont le développeur, c'est-à-dire une personne ou un groupe de personnes qui conçoit et développe le code informatique faisant fonctionner le système et qui en assure la maintenance, et l'opérateur de nœud (Taxonomie, par. 176). En résumé, la couche « infrastructure » fournit à l'entreprise la technologie des registres distribués.

Responsabilité de la gestion de la continuité des opérations et des normes de service

48. La *gestion de la continuité des opérations* est le processus qui consiste à faire en sorte qu'une entité puisse continuer de fonctionner en cas de catastrophe, de perturbation ou d'événement inattendu. Il s'agit notamment de déceler les menaces et les faiblesses potentielles, d'élaborer et de mettre en œuvre des plans visant à atténuer ou à prévenir ces menaces, ainsi que de mettre ces plans à l'essai et d'en assurer le maintien pour en garantir l'efficacité. La *gestion des niveaux de service* est le processus qui consiste à définir, approuver et mesurer les résultats et la qualité des services qu'une entité fournit à sa clientèle. Il s'agit notamment de fixer des objectifs concernant les niveaux de service, de contrôler ces niveaux et, si nécessaire, de prendre des mesures correctives pour veiller à ce qu'ils soient atteints.

49. La continuité des opérations et une bonne gestion des niveaux de service sont essentielles pour instaurer la confiance dans l'utilisation des registres distribués. Pour les entreprises qui souhaitent utiliser des systèmes de registres distribués dans leurs opérations commerciales, le choix de mettre au point de tels systèmes en interne ou d'en confier la tâche à un développeur tiers dépend de l'ampleur des opérations en question. Une entreprise suffisamment importante peut développer son propre système de registre distribué. Si l'entreprise entend exploiter le système et en proposer l'utilisation ou l'accès à des tiers, elle peut alors avoir la responsabilité de maintenir un certain niveau de services en tant que développeur, opérateur, ou les deux.

50. Lorsqu'elles externalisent leurs systèmes de registres distribués, les entreprises doivent s'assurer que le développeur dispose de plans de gestion de la continuité des opérations et qu'un niveau de services minimum est respecté. Il est recommandé de faire preuve de diligence raisonnable lors de l'évaluation de ces questions, laquelle peut avoir lieu lors du contrôle préalable des contreparties, mais aussi au cours de la prestation de services. À cet effet, il est possible de demander au développeur de fournir ses antécédents ainsi que des bilans ou des états de la performance financière permettant d'évaluer sa situation financière, et d'effectuer une recherche basique en ligne sur sa réputation et son importance.

51. Les entreprises peuvent envisager de conclure des contrats avec des développeurs pour définir des plans de gestion de la continuité des opérations et la norme minimale de service attendue. Elles peuvent en outre envisager d'adopter des lignes directrices ou des politiques internes sur les normes minimales que les prestataires de services tiers doivent respecter pour qu'il soit possible de conclure un contrat avec eux. Il peut être nécessaire de modifier les clauses existantes en matière de gestion de la continuité des opérations pour les adapter aux caractéristiques de la technologie des registres distribués. Une diligence raisonnable, associée à un contrat qui définit clairement les droits et obligations des parties, peut réduire les risques d'inexécution de la part du prestataire de services.

Procédures d'audit et droit d'audit

52. Une question liée à la relation entre le prestataire de services et l'utilisateur est le droit de procéder à des audits et la mise en œuvre des procédures y relatives. La conduite d'audits sur le code du registre, le développeur et l'opérateur par des tiers indépendants peut renforcer la confiance dans le système de registre distribué

déployé. Les procédures d'audit peuvent consister à procéder à l'*audit du registre distribué* afin d'éliminer les codes dysfonctionnels ou frauduleux et de détecter les éventuelles failles ou faiblesses du système.

53. Lorsque les entreprises externalisent la conception du registre distribué ou son exploitation, elles peuvent envisager d'insérer dans le contrat conclu avec le développeur et l'opérateur une clause en vertu de laquelle elles peuvent réaliser un audit du code. Cela leur donne le droit contractuel de mener leurs propres audits du code du développeur tiers. Le code étant essentiellement destiné à être exécuté dans les propres serveurs ou systèmes informatiques des entreprises, le droit d'audit et la conclusion d'un accord sur les modalités de cet audit sont des mécanismes importants pour ce qui est de protéger les entreprises contre les cyberattaques exploitant les erreurs qu'il pourrait contenir.

Préoccupations environnementales

54. Dans le mécanisme de consensus par preuve de travail, sur lequel reposent les cryptomonnaies telles que le bitcoin, la vérification du fait que les transactions ont été exécutées dans le registre distribué implique une forte consommation d'énergie. Les organismes de réglementation s'inquiètent de l'empreinte écologique du *minage* des registres distribués[15]. Il est souhaitable de réduire la consommation électrique induite par le mécanisme de preuve de travail, et plusieurs initiatives visent à décarboniser le secteur des cryptomonnaies[16]. Le passage d'un mécanisme de consensus par preuve de travail à un mécanisme de preuve par l'enjeu pourrait réduire les coûts énergétiques liés au cryptominage[17].

55. Compte tenu de la grande quantité d'électricité consommée pour le minage des registres distribués, il se peut à l'avenir que les exigences en matière de réglementation ou de déclaration des activités concernées se multiplient et que leur portée s'élargisse. Les entreprises qui pratiquent le minage devraient connaître la législation susceptible de régir ces activités[18].

F. Questions relatives à la couche « applications »

56. La couche « applications » de la technologie des registres distribués se rapporte à l'offre de produits et de services. Les acteurs concernés sont l'entreprise qui propose les produits et services et les utilisateurs de ces derniers.

Automatisation des contrats

57. Les contrats automatisés basés sur la technologie des registres distribués ont été présentés comme l'un des atouts majeurs des systèmes de registres distribués en raison du degré de confiance accru dans l'exécution automatisée du code (voir par. 24 ci-dessus). Le projet de dispositions de la CNUDCI relatives aux contrats automatisés (A/CN.9/1178 et A/CN.9/1179) contient des orientations technologiquement neutres sur les questions juridiques susceptibles de se poser lors du recours à l'automatisation

[15] Pour plus d'informations sur les incidences environnementales du minage des registres distribués, voir Chamanara, S. et Madani, K. (2023). The Hidden Environmental Cost of Cryptocurrency: How Bitcoin Mining Impacts Climate, Water and Land, Institut pour l'eau, l'environnement et la santé de l'Université des Nations Unies (UNU-INWEH), Hamilton, Ontario (Canada), https://inweh.unu.edu/.

[16] Par exemple, le *Crypto Climate Accord* (accord sur les cryptomonnaies et le climat) est une initiative de décarbonisation du minage des registres distribués.

[17] Le réseau Ethereum est passé du mécanisme de preuve de travail au mécanisme de preuve par l'enjeu, ce qui a considérablement réduit la consommation d'énergie et l'empreinte carbone.

[18] Par exemple, aux États-Unis, la loi de 2022 sur la transparence environnementale des cryptoactifs (*Crypto-Asset Environmental Transparency Act*) impose aux parties qui consomment plus de cinq mégawatts d'électricité dans le cadre d'opérations de cryptominage de déclarer leurs émissions de dioxyde de carbone conformément à la loi sur la lutte contre la pollution atmosphérique (*Clean Air Act*).

des contrats. Il ne traite pas de la probabilité d'exécution du script, qui est une considération commerciale et non juridique. Il ne s'intéresse pas non plus à la manière d'automatiser certaines clauses contractuelles (voir par. 39 et 40 ci-dessus).

Responsabilité en cas d'informations incorrectes

58. Un aspect de la responsabilité et de la répartition des risques a trait aux cas où les informations contenues dans le registre distribué sont inexactes, que la cause en soit une erreur de bonne foi ou un comportement frauduleux. Cela peut se produire au stade du développement (par exemple, insertion d'un code malveillant lors du déploiement du registre) ou lors de la saisie d'informations (par exemple, saisie d'informations dont on sait qu'elles sont inexactes) (voir par. 20 ci-dessus).

59. En ce qui concerne la saisie de données, la responsabilité de l'enregistrement d'informations inexactes ou fausses est imputée à la personne qui a fourni les informations ou au nom de laquelle celles-ci ont été fournies. D'un point de vue commercial, les entreprises devraient examiner attentivement la qualité des données saisies et les mesures correctives possibles, en particulier si elles se servent du registre distribué pour des opérations cruciales. Celles qui autorisent des utilisateurs, en particulier des tiers, à accéder à leur registre distribué privé avec permission ou à l'utiliser devraient établir une relation contractuelle afin de limiter leur responsabilité à l'égard desdits utilisateurs.

Confidentialité et protection des données

60. De nombreux États ont adopté des lois sur la confidentialité et la protection des données qui s'appliquent également aux applications basées sur la technologie des registres distribués. Par exemple, le Règlement général de l'UE sur la protection des données (« RGPD »)[19] s'applique dès lors que des données à caractère personnel sont en jeu, y compris quand cette technologie est utilisée. Il a été avancé à cet égard qu'une clef publique pouvait être considérée comme une donnée à caractère personnel au sens du RGPD, compte tenu des analogies entre clefs publiques et adresses IP dynamiques[20].

61. Lorsqu'elles mettent en œuvre des registres distribués, les entreprises doivent se demander si des données à caractère personnel y seront stockées et prendre activement des mesures pour se conformer aux lois applicables en matière de confidentialité et de protection des données. Le développeur, l'opérateur et l'utilisateur pouvant se trouver dans plusieurs pays, il convient d'insérer des clauses contractuelles dans l'accord de services afin de garantir la conformité avec l'ensemble desdites lois.

Stockage des données (« droit à l'oubli » et « droit à l'effacement »)

62. La persistance des informations enregistrées dans des registres distribués peut poser des difficultés en ce qui concerne le respect de certains droits tels que le *droit à l'oubli* et le *droit à l'effacement*. Ces questions sont d'autant plus pertinentes lorsque les données ou les informations en question sont des données à caractère personnel très sensibles, telles que des dossiers médicaux ou des informations biométriques. En outre, du fait de la nature décentralisée de la technologie des registres distribués, les informations personnelles d'une personne résidant dans un

[19] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119, 4.5.2016, p. 1 à 88, ELI : http://data.europa.eu/eli/reg/2016/679/oj.

[20] En ce qui concerne l'application du RGPD aux adresses IP dynamiques, voir Cour de justice européenne, 19 octobre 2016, *Patrick Breyer* c. *Bundesrepublik Deutschland*, ECLI :EU :C :2016 :779.

pays peuvent être stockées dans un autre, et le lieu de stockage peut changer régulièrement.

63. Par ailleurs, en raison de cette nature décentralisée, il peut être difficile d'identifier un responsable du traitement des données ou une autre entité chargée de faire respecter le « droit à l'oubli » et le « droit à l'effacement ». L'utilisation de pseudonymes peut compliquer encore la tâche.

64. Sur le plan conceptuel, on peut objecter que la technologie des registres distribués n'est pas toujours strictement immuable et que les développeurs et les administrateurs peuvent convenir de supprimer certaines données, à tout le moins dans les registres privés avec permission. Toutefois, cette solution ne règle pas la question de la suppression des données figurant dans des registres publics sans permission.

65. Une autre solution pourrait consister à stocker les données à caractère personnel dans une base de données distincte du registre distribué. Cette option ne résout cependant pas le problème du droit à l'effacement et peut entraîner une augmentation des coûts.

66. Les plateformes de registres distribués peuvent aussi adopter des fonctions d'amélioration de la confidentialité qui permettent de chiffrer ou d'anonymiser les données, de sorte que ces dernières ne puissent pas être facilement rattachées à une personne. Toutefois, ces mesures ne suffisent pas toujours à protéger pleinement les données à caractère personnel. En outre, la préservation de la confidentialité de la transaction ne doit pas altérer son caractère vérifiable. Lorsque ces fonctions d'amélioration de la confidentialité ne peuvent pas être mises en œuvre, par exemple en raison de l'utilisation d'un registre public sans permission, il serait possible d'appliquer le principe de la minimisation des données dans le traitement des informations sur le réseau (voir par. 69 ci-dessous).

Droit de modifier les informations stockées à tort

67. Un autre problème opérationnel lié à la persistance des données est qu'il peut être difficile de modifier des informations stockées qui sont incorrectes ou de mettre à jour ou de remplacer des données qui ne sont plus pertinentes ou exactes. Un moyen de contourner le problème consisterait à appliquer le droit à l'oubli, c'est-à-dire à mettre en place des règles de gouvernance prédéfinies et à réduire la centralisation au profit du contrôle des données.

68. Un code permettant la modification ou la suppression de données à la demande de l'utilisateur a été publié. Cette solution technique offre aux entreprises une possibilité supplémentaire de se conformer à la loi sur la confidentialité et la protection des données.

Mesures d'atténuation

69. Pour limiter les problèmes susmentionnés, les entreprises peuvent recourir à des dispositifs d'amélioration de la confidentialité tels que les *preuves à divulgation nulle de connaissance*. Il s'agit d'une méthode permettant à une partie (le « fournisseur de preuve ») de prouver à une autre partie (le « vérificateur ») qu'une proposition donnée est vraie sans communiquer d'autre information que le fait que la proposition est effectivement vraie.

70. Les entreprises peuvent envisager de chiffrer et d'anonymiser les données afin qu'il ne soit pas aisé de les relier à une personne. Si ces données sont perdues et retrouvées ensuite par une personne qui n'est pas en possession de la clef de déchiffrement, elles seront inutilisables.

Applications spécifiques : actifs numériques

71. Le traitement juridique des données stockant de la valeur, qui sont généralement connues sous le nom d'« actifs numériques », fait l'objet d'une attention particulière. Bien que toute donnée ait une certaine valeur et puisse donc entrer dans la définition de l'actif numérique, la notion juridique d'« actif numérique » renvoie souvent au stockage et au transfert de valeur à l'aide de la technologie des registres distribués. Les États la définissent selon différentes approches. Ainsi, la Commodity Futures Trading Commission (« CFTC ») des États-Unis d'Amérique semble mettre l'accent sur le contrôle et la transférabilité des actifs numériques[21], tandis que l'Union européenne paraît s'attacher à ce que l'actif « représente », c'est-à-dire les droits matérialisés par le jeton[22]. La Taxonomie reconnaît l'absence de consensus sur la définition du terme « actif numérique » ; elle indique toutefois que dans son sens habituel, ce terme désigne un ensemble de données, stockées électroniquement, qui sont utiles ou qui ont une valeur (Taxonomie, par. 82).

72. Des lois ont été élaborées afin de combler les lacunes juridiques du régime applicable aux actifs numériques[23]. Certaines garantissent l'application d'autres lois, en particulier celle applicable aux documents commerciaux et aux monnaies. En ce qui concerne le droit international privé, le Bureau Permanent de la HCCH mène une étude *lex specialis* portant sur les questions de droit international privé soulevées par des cas concrets d'utilisation transfrontière de jetons numériques[24].

73. Les applications concernant les actifs numériques qui font intervenir la technologie des registres distribués étant très diverses, il est souhaitable d'examiner séparément les questions juridiques soulevées par les différents types d'actifs numériques.

Services de paiement et cryptomonnaies

74. Les actifs numériques peuvent être utilisés pour transférer de la valeur[25]. On parle alors souvent de « cryptomonnaies ». Les cryptomonnaies peuvent avoir une valeur marchande si elles sont suffisamment liquides pour être échangées sur des marchés prévus à cet effet (les *« plateformes d'échange de cryptomonnaies »*). La valeur de certaines est liée à de la monnaie fiduciaire ou à d'autres biens afin d'atténuer la volatilité (« *monnaie numérique stable* »).

75. Les cryptomonnaies peuvent être considérées comme une forme plus stable et plus efficace de transfert de valeur lorsque les monnaies nationales sont très volatiles ou que des restrictions sur les paiements transfrontières sont en place. Dans certains États, elles ont été déclarées comme ayant cours légal, parallèlement à la monnaie nationale. Cela a toutefois soulevé de nouvelles questions, par exemple sur le taux de change entre la monnaie préexistante et la cryptomonnaie et, plus généralement, sur la politique monétaire.

76. L'utilisation des cryptomonnaies soulève des enjeux de nature juridique, réglementaire et commerciale. La qualification juridique d'une cryptomonnaie et, partant, le régime réglementaire applicable dépendent de ses caractéristiques. Les organismes de réglementation considèrent de plus en plus les actifs numériques

---

[21] CFTC, Digital Asset Markets Subcommittee Recommendation – Adoption of an Approach for the Classification and Understanding of Digital Assets (recommandation du sous-comité des marchés d'actifs numériques – adoption d'une méthode de classification et d'appréhension des actifs numériques), 7 mars 2024.

[22] Global Blockchain Business Council, Regulatory Map (carte des réglementations).

[23] Aux États-Unis, article 12 du Code de commerce uniforme ; Principes d'UNIDROIT sur les actifs numériques et le droit privé ; loi nº 2 de 2024 sur les actifs numériques du Dubai International Financial Centre.

[24] HCCH, C&D de mars 2024, nº 12.

[25] La création du bitcoin avait pour objectif initial de permettre des paiements décentralisés.

comme des matières premières, des valeurs mobilières ou les deux[26]. Les services de paiement effectués à l'aide de la technologie des registres distribués sont soumis au droit des paiements.

77. Sur le plan juridique, une question non encore résolue est celle de savoir si les cryptomonnaies peuvent être classées dans la catégorie des biens. Dans les pays où cela est possible, les détenteurs de cryptomonnaies peuvent utiliser les voies de droit ouvertes aux propriétaires, par exemple le gel d'un actif[27].

78. D'un point de vue commercial, les cryptomonnaies, y compris les monnaies numériques stables, peuvent être très volatiles. Si les entreprises souhaitent effectuer des paiements en cryptomonnaies, elles peuvent envisager d'utiliser différentes plateformes d'échange de cryptomonnaies et différentes cryptomonnaies afin d'atténuer les risques qui pourraient survenir en cas de problème lié à la plateforme ou à la monnaie, par exemple en cas de défaillance soudaine de la plateforme.

79. Les monnaies numériques des banques centrales (ci-après « MNBC ») sont définies comme de la monnaie fiduciaire émise sous forme électronique. À ce titre, elles sont émises uniquement par les banques centrales et leur nature diffère de celle des cryptomonnaies[28]. Les projets pilotes les concernant, qui font souvent intervenir la technologie des registres distribués[29], portent essentiellement sur leur utilisation dans le commerce de détail[30]. La HCCH a créé un Groupe d'experts sur les questions de loi applicable et de compétence qui se posent dans le cadre de l'utilisation et du transfert transfrontières de MNBC[31].

Documents transférables électroniques

80. Dans la pratique, les documents transférables électroniques, tels que définis dans la LTDTE, peuvent être émis au moyen d'applications basées sur la technologie des registres distribués. Il s'agira de documents et d'instruments transférables sous forme électronique qui, à ce titre, seront régis par le droit matériel qui leur est applicable et par les dispositions de la LTDTE. La note explicative relative à la LTDTE contient des orientations précises sur certaines questions relatives à la technologie des registres distribués. Par exemple, dans les systèmes dépourvus d'opérateur central, le consentement à l'utilisation de documents transférables électroniques peut être implicite et se déduire de circonstances telles que l'exercice du contrôle sur le document ou l'exécution de l'obligation prévue dans le document en question (note explicative relative à la LTDTE, par. 66). En outre, lorsque des pseudonymes sont utilisés, l'exigence d'identification de la personne qui a le contrôle

---

[26] Dans certains cas, les cryptomonnaies peuvent être qualifiées de documents commerciaux. Par exemple, une monnaie numérique stable indexée sur le cours d'une matière première (c'est-à-dire dont la valeur est liée à une matière première donnée) peut être qualifiée de récépissé d'entrepôt si la matière première est identifiée et stockée dans un entrepôt (par opposition à un indice des prix des produits de base) et si les autres exigences légales d'un récépissé d'entrepôt sont remplies.

[27] Par exemple, dans l'affaire *AA* c. *X* [2019] EWHC 3556 (Comm), un tribunal anglais a autorisé une injonction de propriété concernant des bitcoins dans le cadre du paiement d'une rançon. La localisation et le recouvrement civils d'actifs, y compris numériques, dans les procédures d'insolvabilité constituent un axe spécifique des travaux de la CNUDCI (voir A/CN.9/WG.V/WP.192 et A/CN.9/WG.V/WP.193).

[28] Le Fonds monétaire international a publié un manuel virtuel sur les MNBC, lequel fournit des informations sur les questions les plus fréquemment posées en la matière par les décideurs. Ce manuel offre également aux utilisateurs un cadre pour étudier ces monnaies et contient un chapitre consacré à leur conception. Il est disponible à l'adresse suivante : www.imf.org/en/Topics/fintech/central-bank-digital-currency/virtual-handbook.

[29] Le projet mBridge, par exemple, s'appuie sur un registre distribué spécialement conçu pour les paiements transfrontières dans plusieurs monnaies numériques des banques centrales ; voir www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm.

[30] Il est déjà possible de créer de la monnaie fiduciaire de gros sous forme exclusivement électronique, au moyen d'une entrée dans un registre. Une fois cette monnaie transférée aux banques commerciales, celles-ci ont une dette envers la banque centrale.

[31] HCCH, C&D de mars 2024, n^{os} 9 et 10.

peut être satisfaite par l'association du pseudonyme et du nom (note explicative relative à la LTDTE, par. 117).

81. Les mêmes considérations s'appliquent à l'émission de documents électroniques transférables en vertu d'une loi qui ne prévoit pas d'approche fondée sur l'équivalence fonctionnelle mais qui autorise l'utilisation de ces documents sous forme électronique uniquement. De même, elles valent pour une loi qui autorise l'utilisation de documents papier et électroniques en adoptant une approche neutre quant au support. Le projet de loi type CNUDCI-UNIDROIT sur les récépissés d'entrepôt (A/CN.9/1182) illustre cette dernière approche.

G. Questions relatives à la couche « gouvernance »

82. En raison de la nature décentralisée de la technologie des registres distribués, des questions particulières liées à la gouvernance peuvent se poser en ce qui concerne la couche « infrastructure », notamment dans le cas des registres distribués publics sans permission. La cause en est l'absence d'autorité centrale, les décisions étant normalement prises par un vote basé sur des jetons de gouvernance. Les détenteurs de ces jetons peuvent ne pas connaître l'existence des autres détenteurs, voire ne pas être identifiés puisqu'ils opèrent sous un pseudonyme. Il s'agit de la couche « gouvernance ».

83. Il n'est pas rare que des procédures judiciaires soient engagées contre les acteurs de la couche « gouvernance ». Bien que ce type de procédure puisse généralement porter sur toute question liée au dysfonctionnement du système de registre distribué, dans la pratique, les affaires portées devant les tribunaux concernent souvent la perte d'actifs numériques due à l'exploitation d'erreurs de programmation par des pirates informatiques. Comme il est souvent impossible, pour des raisons pratiques, de poursuivre les pirates en justice, les parties lésées demandent réparation aux acteurs de la couche de gouvernance présumés responsables des erreurs de programmation.

84. De manière générale, la possibilité d'intenter une action contre les opérateurs de nœuds, les développeurs ou les membres d'organisations autonomes décentralisées (voir par. 98 ci-dessous) dépend du type de registre distribué et de ses objectifs. Une répartition des rôles peut faciliter l'examen des profils de responsabilité. Il existe essentiellement quatre rôles clefs à prendre en compte lorsqu'il est question de la responsabilité dans le domaine de la technologie des registres distribués : les développeurs du code, les opérateurs du registre, les utilisateurs du registre et les parties qui demandent des dommages-intérêts. Les signatures électroniques reposant sur la cryptographie sont utilisées pour établir les rôles liés à un pseudonyme.

85. L'un des principaux problèmes liés à l'utilisation d'une structure de gouvernance décentralisée est qu'il peut être compliqué de s'accorder sur les droits et les obligations de chaque partie, en particulier dans le cas des registres distribués publics sans permission, en raison de l'incertitude concernant la reconnaissance des structures de ce type en tant que personnes morales. Bien souvent, il est même difficile d'identifier les entités concernées en raison de l'utilisation d'un pseudonyme.

86. Il est possible de réduire les risques de contrepartie en incitant les développeurs à élaborer des registres distribués privés avec permission. La contrepartie étant alors clairement identifiée, les entreprises peuvent faire preuve de diligence raisonnable, par exemple en s'assurant de conclure un contrat avec une entité légalement reconnue et en vérifiant les antécédents de la société en matière d'élaboration et de maintenance de systèmes de registres distribués.

87. Les entreprises qui se servent de registres distribués privés avec permission à des fins commerciales rencontrent généralement moins de difficultés en cas d'action contre un développeur, car elles sont sûres de l'identité de ce dernier et des conditions dans lesquelles le code a été conçu et déployé.

88. En revanche, les actions visant les développeurs d'un registre distribué public sans permission peuvent être plus complexes. Premièrement, l'identification des développeurs ou des opérateurs de nœuds qui opèrent sous un pseudonyme peut demander des efforts considérables. Deuxièmement, on peut s'interroger sur l'existence et la nature (obligation fiduciaire, par exemple) d'une éventuelle relation juridique établie pour définir les droits et obligations qui existent entre la partie lésée et le développeur ou l'opérateur[32]. Troisièmement, l'éloignement géographique peut compliquer l'exécution des jugements prononcés contre des développeurs ou des opérateurs de nœuds.

89. En outre, il peut être difficile de déterminer la personnalité juridique du développeur ou de l'opérateur (par exemple, dans le cas d'une organisation autonome décentralisée), ce qui rend délicate l'attribution de la responsabilité aux parties concernées. Les entreprises peuvent atténuer les risques en souscrivant une couverture d'assurance, s'il en existe une qui soit applicable à leurs activités commerciales.

90. La responsabilité des développeurs concernant les registres distribués publics sans permission est mise en cause dans les procédures intentées contre des développeurs de cryptomonnaies. Dans une affaire, un propriétaire de bitcoins ayant perdu des actifs à la suite du piratage de son compte a poursuivi les développeurs du bitcoin pour qu'ils mettent au point un correctif logiciel permettant de rétablir l'accès au compte, en invoquant une obligation fiduciaire entre les développeurs et les utilisateurs[33]. Il a été constaté que l'argument selon lequel les développeurs avaient une obligation fiduciaire à l'égard des utilisateurs pouvait être valable[34].

Organisations autonomes décentralisées

91. Les systèmes de registres distribués ont inspiré la création d'une entité particulière appelée « organisation autonome décentralisée », chargée d'en assurer la gouvernance. Les organisations autonomes décentralisées sont une structure de gouvernance fondée sur la technologie des registres distribués que toute organisation, à but lucratif ou non, peut utiliser. Plusieurs gouvernements et institutions en ont donné une définition ; par exemple, la Banque centrale européenne a défini les organisations autonomes décentralisées comme des « organisations virtuelles dont la création et le fonctionnement reposent sur un code informatique et sur la technologie de la chaîne de blocs ». D'autres institutions ont livré des définitions plus détaillées : ainsi, le Département du Trésor des États-Unis définit ces organisations comme « un système d'administration qui fonctionne selon un ensemble de règles ou de contrats intelligents codés et transparents ».

92. On peut dégager des éléments clefs communs aux organisations autonomes décentralisées. Celles-ci utilisent des contrats automatisés reposant sur la technologie des registres distribués. Elles sont généralement décentralisées et comptent plusieurs membres situés dans différents pays. La structure de gouvernance et le statut juridique d'une organisation autonome décentralisée sont donc des questions importantes lorsqu'il s'agit d'établir une relation contractuelle ou de répartir la responsabilité entre les parties.

---

[32] Pour combler cette lacune, il a été suggéré d'engager des actions en vertu du droit de la responsabilité du fait des produits dans les pays où ces actions ne portent pas seulement sur les dommages corporels, mais couvrent aussi les pertes financières (https://jonasgross.medium.com/legal-aspects-of-blockchain-technology-liability-8f5b433030f). Dans ces cas, c'est souvent aux développeurs, mais rarement aux opérateurs, que l'on cherche à imputer la responsabilité du fait des produits dans le contexte de la technologie des registres distribués.

[33] *Tulip Trading* c. *Bitcoin Association*, 25 mars 2022, [2022] EWHC 667 (Ch).

[34] Le demandeur a contesté la décision de la juge Falk dans l'affaire *Tulip Trading* c. *Bitcoin Association* et il a été accueilli en appel. L'affaire sera jugée en vue de déterminer si l'obligation fiduciaire existe en l'espèce : voir l'arrêt d'appel du juge Lewison, du juge Popplewell et du juge Birss, *Tulip Trading* c. *Van der Laan*, 3 février 2023, [2023] EWCA Civ 83.

93. La forme variable et la nature décentralisée des organisations autonomes décentralisées font qu'elles peuvent adopter des structures de gouvernance hybrides[35]. Il importe donc de décrire la structure de gouvernance de ces organisations afin d'examiner les questions juridiques qui en découlent. L'incapacité de conférer de façon adéquate la personnalité juridique à une organisation autonome décentralisée a des conséquences notables pour les entreprises qui effectuent des transactions avec des organisations de ce type et pour les membres de ces dernières, lesquels peuvent être tenus personnellement responsables des actions de l'organisation.

Structure de gouvernance des organisations autonomes décentralisées

94. Les organisations autonomes décentralisées peuvent adopter différentes structures organisationnelles. La prise de décision peut être réservée aux fondateurs de l'organisation, être automatisée au moyen de protocoles logiciels ou relever d'un système de voix pondérées en fonction du type et du nombre de jetons contrôlés. Les organisations autonomes décentralisées se servent de contrats automatisés basés sur la technologie des registres distribués pour définir les règles relatives à l'objectif de l'organisation et à la manière dont les membres conviennent de coopérer, dont les décisions sont prises collectivement dans le cadre d'un processus de vote, dont les jetons natifs sont créés et distribués et dont les transactions sont exécutées une fois certaines conditions remplies.

95. La structure de gouvernance d'une organisation autonome décentralisée repose sur des contrats automatisés basés sur la technologie des registres distribués, d'où la nécessité d'un processus décisionnel structuré. En l'absence d'autorité centrale, il est capital de disposer de mécanismes de consensus et de règlement des différends (vote à la majorité ou algorithmes, par exemple). La première étape consiste à déterminer qui peut soumettre une proposition d'action. Ensuite, un organe de décision ou un algorithme prend une décision.

96. Certaines organisations n'autorisent que les membres détenant un certain type d'actif numérique (appelé « jeton de gouvernance ») à participer aux processus décisionnels. Souvent, le poids d'une voix est proportionnel au montant de l'actif numérique en question détenu. Un moyen fréquent d'obtenir ces actifs numériques consiste à investir dans l'organisation, à lui allouer du temps de travail ou à la soutenir d'autres manières (par exemple en tant qu'ambassadeur commercial).

97. Contrairement aux mécanismes institutionnels classiques, où les décisions sont prises par un conseil d'administration ou des directeurs généraux, les décisions des organisations autonomes décentralisées reposent généralement sur le consensus du groupe ou le vote des membres. Ces organisations sont généralement libres de définir leur structure de gouvernance pour répondre à leurs objectifs, ce qui fait d'elles un outil flexible adapté à des fins collaboratives très diverses. Toutefois, des données empiriques préliminaires montrent que les jetons de gouvernance sont attribués de manière disproportionnée aux fondateurs et aux principaux développeurs.

98. Habituellement, la gouvernance des organisations autonomes décentralisées est fondée sur des règles ou des codes de conduite, que le public peut consulter dans des livres blancs, sur des sites Web ou grâce à des applications. Toutefois, ces règles n'ont pas la même force obligatoire que les outils organisationnels traditionnellement utilisés par les entreprises.

99. Dans certaines organisations autonomes décentralisées, les membres utilisent des pseudonymes. Les principes généraux relatifs au pseudonymat et à l'identification des parties s'appliquent également à ces organisations.

[35] Les structures de gouvernance hybrides permettent un certain degré de centralisation tout en intégrant des éléments de décentralisation. D'un point de vue commercial, il peut s'agir de permettre aux utilisateurs de peser sur certaines décisions de l'entreprise, par exemple la conception de nouveaux produits et leur actualisation.

100. Les caractéristiques typiques d'une organisation autonome décentralisée, dont certaines peuvent présenter des risques pour les entreprises, sont les suivantes :

a) Prise de décision : les règles de consensus sont généralement définies à un stade précoce puis deviennent relativement difficiles à modifier à mesure que l'organisation se développe et se complexifie, ce qui peut se traduire par un mécanisme de consensus inadéquat, c'est-à-dire lent et inefficace. Cela peut, à terme, entraver le fonctionnement de l'organisation voire empêcher une réaction rapide face aux situations imprévues ;

b) Manque de responsabilité : les décisions prises dans une organisation autonome décentralisée associent souvent de nombreuses parties, ce qui entraîne une dilution de la responsabilité, une notion connue en psychologie sociale qui conduit les personnes à se sentir moins responsables. Par conséquent, en raison d'une responsabilité restreinte, les organisations dépourvues de contrôle centralisé risquent de mal gérer les ressources ;

c) Manque de représentation : selon le système de représentation mis en œuvre, par exemple un système de droits de vote proportionnels à la détention d'un actif numérique particulier, certains membres de l'organisation peuvent se sentir sous-représentés dans le processus décisionnel, ce qui peut les amener à moins accepter les décisions et être source de mécontentement et de conflits ;

d) Failles de sécurité : les organisations autonomes décentralisées s'appuient sur des contrats automatisés basés sur la technologie des registres distribués qui sont relativement difficiles à modifier lorsqu'une faille de sécurité est détectée. Elles risquent donc d'être exposées à des cybermenaces ou à des problèmes fondamentaux, par exemple en cas de mécanisme de vote ou de paiement défectueux.

101. Les entreprises qui décident de réaliser des transactions commerciales avec une organisation autonome décentralisée doivent avoir conscience de ces risques. Il est possible de limiter les risques liés à la collaboration avec une de ces organisations, notamment en vérifiant son statut de société et en lui imposant d'identifier ses membres et ses développeurs afin que l'entreprise puisse engager une action fondée sur la responsabilité personnelle si les choses devaient tourner au plus mal.

Obligations contractuelles et questions de responsabilité applicables aux organisations autonomes décentralisées

102. Les organisations autonomes décentralisées peuvent intéresser les entreprises en raison des possibilités de transparence et de personnalisation qu'elles offrent. Cependant, elles s'accompagnent aussi de problèmes potentiels : leur structure organisationnelle non définie crée une forte insécurité juridique. En raison de la diversité des types et des structures possibles d'organisations autonomes décentralisées, il faut évaluer chaque organisation au cas par cas pour déterminer quelle loi s'applique.

103. En l'absence de législation spécifique, des tentatives ont été faites pour classer ces organisations dans un type d'entité juridique existante, telle qu'une société en nom collectif, une société à responsabilité limitée ou une organisation à but non lucratif.

104. Certains États ont adopté des mécanismes juridiques spécifiques (parfois appelés « enveloppes juridiques ») pour doter les organisations autonomes décentralisées d'une personnalité juridique, par exemple en autorisant leur immatriculation[36]. Ces dispositions législatives sont censées assurer la protection

[36] Aux États-Unis, par exemple dans le Tennessee : *Tennessee Code Annotated*, titre 48, tel que modifié ; dans le Vermont : *Blockchain-Based Limited Liability Companies* (sociétés à responsabilité limitée fondées sur la technologie de la chaîne de blocs), *V.S.A.*, chap. 11, par. 4173 ; et dans le Wyoming : *Wyoming Decentralized Unincorporated Nonprofit Association Act* (loi du Wyoming sur les associations à but non lucratif décentralisées sans personnalité

d'une entité juridique et permettre à ces organisations de limiter leur responsabilité à l'instar d'une société à responsabilité limitée[37]. La prévisibilité juridique s'en trouve considérablement accrue, ce qui simplifie les relations commerciales avec les organisations autonomes décentralisées.

105. Dans les États où les organisations autonomes décentralisées peuvent être constituées en société, pour celles qui ne l'ont pas été, les organismes de réglementation ont cherché à faire porter la responsabilité sur les membres individuels et à les tenir personnellement responsables[38]. Sur le plan juridique, cela entraîne généralement la responsabilité personnelle illimitée des « partenaires » (c'est-à-dire les détenteurs de jetons) de l'organisation.

106. Toutefois, d'un point de vue pratique, la poursuite à titre individuel des membres d'une organisation autonome décentralisée peut s'avérer longue et difficile, en particulier si ces derniers utilisent des pseudonymes et ne résident pas dans le même État.

107. La qualification juridique d'une organisation autonome décentralisée détermine le régime d'insolvabilité applicable. Toutefois, la nature de l'organisation et le recours à la technologie des registres distribués peuvent soulever des questions particulières en matière d'insolvabilité. Par exemple, les membres de l'organisation peuvent être considérés comme des créanciers ou, au contraire, comme des débiteurs de l'organisation insolvable ; les jetons de gouvernance peuvent être considérés comme des biens ; les membres et les administrateurs, s'il en existe, peuvent être considérés comme ayant des obligations fiduciaires les uns envers les autres et envers les utilisateurs, etc.

Loi type de la Coalition d'applications légales automatisées

108. Plusieurs institutions universitaires ont mené des projets visant à régler les questions juridiques liées aux organisations autonomes décentralisées. La Coalition d'applications légales automatisées (« COALA ») est un groupe de réflexion qui étudie les questions juridiques soulevées par l'économie décentralisée et la technologie des registres distribués. Elle a publié une loi type sur les organisations autonomes décentralisées (« loi type de la COALA ») qui contient des règles applicables à la gouvernance et au fonctionnement de ces organisations[39].

109. La loi type de la COALA adapte le concept d'équivalence fonctionnelle au contexte des organisations autonomes décentralisées. Elle indique que l'établissement de l'équivalence fonctionnelle est « utile pour simplifier la réglementation des organisations autonomes décentralisées » et que cela nécessite « de définir un objectif ou un but et de démontrer ensuite que cet objectif ou ce but pourrait être atteint soit par l'application d'une règle juridique, soit au moyen d'une application particulière

---

juridique), *Wyoming Statutes*, titre 17, chap. 32. Voir également la loi de 2022 sur les organisations autonomes décentralisées (*Decentralized Autonomous Organization Act*) de la République des Îles Marshall.

[37] Par exemple, le Vermont autorise l'immatriculation d'une « société à responsabilité limitée fondée sur la technologie de la chaîne de blocs », qui exige que la société concernée indique « si la base de données ou le registre fondé sur le consensus et décentralisé qu'elle utilise ou dont elle permet le fonctionnement sera entièrement décentralisé ou partiellement décentralisé et si cette base de données ou ce registre sera entièrement ou partiellement public ou privé » (*Vermont Statutes Annotated*, chap. 11, par. 4173).

[38] *Commodity Futures Trading Commission* c. *Ooki DAO*, United States District Court, Northern District of California, affaire nº 3 :22-cv-05416-WHO. Le tribunal a estimé que « l'organisation autonome décentralisée Ooki [était] une "personne" au sens de la loi sur les bourses de marchandises (*Commodity Exchange Act*) et qu'elle [pouvait] donc être tenue responsable des infractions à la loi ». Le tribunal a ensuite jugé que l'organisation avait effectivement enfreint la loi comme il était allégué.

[39] Aux États-Unis, la loi de l'Utah sur les organisations autonomes décentralisées (*Utah Decentralized Autonomous Organizations Act*) (*Utah Code*, titre 48, chap. 5) s'inspire de la loi type de la COALA.

de la technologie »[40]. En ce qui concerne l'équivalence fonctionnelle, elle donne l'exemple suivant :

> « Par exemple, au lieu de mettre en place de nouvelles règles d'entreprise spécifiquement applicables aux actions "jetonisées", il serait possible de considérer les actions enregistrées dans un système de chaîne de blocs comme des titres d'actions valides, transférables au moyen d'un registre fondé sur la chaîne de blocs. L'équivalence réglementaire repose sur la même technique mais définit comme objectif l'objet ou le but d'une réglementation donnée. Elle permet d'établir une équivalence entre la fonction d'une règle juridique et la fonction d'une technologie. »[41]

110. La loi type de la COALA résout la question de la personnalité juridique en dotant explicitement les organisations autonomes décentralisées d'une personnalité juridique indépendante et distincte de celle de leurs membres (art. 2 de la loi type de la COALA).

[40] COALA, loi type sur les organisations autonomes décentralisées, p. 8.
[41] Ibid., p. 3.

III. Glossaire

Audit du registre distribué : procédure d'audit destinée à éliminer les codes dysfonctionnels ou frauduleux ou à détecter les éventuelles failles ou faiblesses du système de registre distribué.

Bouton d'arrêt d'urgence (« Kill switch ») : logiciel permettant d'arrêter l'exécution automatique de clauses automatisées.

Consensus : accord entre les nœuds sur la manière dont une transaction est validée dans le registre distribué.

Droit à l'effacement : droit d'une personne de demander à une organisation ou à une entreprise d'effacer les données à caractère personnel la concernant.

Droit à l'oubli : semblable au droit à l'effacement, le droit à l'oubli est le droit d'une personne de demander à une organisation ou à une entreprise d'effacer les données à caractère personnel la concernant, mais en exigeant de surcroît que cette dernière veille à ce que des tiers ne fassent pas référence aux données en question fournies par elle ou ne créent pas de lien vers elles.

Fonction de hachage cryptographique : algorithme qui convertit une chaîne d'entrée en une chaîne de sortie de taille fixe. Cette chaîne de sortie peut être stockée et utilisé ultérieurement à des fins de vérification.

Gestion de la continuité des opérations : processus qui consiste à faire en sorte qu'une entité puisse continuer de fonctionner en cas de catastrophe, de perturbation ou d'événement inattendu. Il s'agit notamment de déceler les menaces et les faiblesses potentielles, d'élaborer et de mettre en œuvre des plans visant à atténuer ou à prévenir ces menaces, ainsi que de mettre ces plans à l'essai et d'en assurer le maintien pour en garantir l'efficacité.

Gestion des niveaux de service : processus qui consiste à définir, approuver et mesurer les résultats et la qualité des services qu'une entité fournit à sa clientèle. Il s'agit notamment de fixer des objectifs concernant les niveaux de service, de contrôler ces niveaux et, si nécessaire, de prendre des mesures correctives pour veiller à ce qu'ils soient atteints.

Jetons non fongibles : type d'actif numérique dont les unités ne sont pas interchangeables.

Mécanisme de consensus : mécanisme permettant de parvenir à un consensus. Les types de mécanismes de consensus les plus courants sont les mécanismes de preuve de travail et de preuve par l'enjeu.

Minage : activité liée à certains mécanismes de consensus, tels que le mécanisme de preuve de travail, et qui consiste à valider les transactions enregistrées dans le registre distribué. Ceux qui participent à cette activité sont des mineurs.

Monnaie numérique stable : type d'actif numérique dont la valeur est adossée à un autre actif. Cet autre actif peut être de la monnaie fiduciaire, des matières premières ou d'autres actifs numériques.

Monnaies numériques des banques centrales : monnaie fiduciaire sous forme électronique.

Opérateur de nœud : opérateur d'un ordinateur faisant partie du réseau d'un registre distribué.

Persistance de l'information (ou *immuabilité*) : caractéristique des registres distribués selon laquelle les données qui y sont enregistrées ne peuvent pas être modifiées ou supprimées après leur enregistrement.

Plateforme d'échange de cryptomonnaies : plateforme de négociation ou marché permettant d'acheter et de vendre des actifs numériques, en fonction de l'offre de chaque plateforme.

Portefeuilles multisignatures (« multisig ») : service utilisant plusieurs clefs privées qui permet de contrôler, de stocker ou de transférer des actifs numériques.

Preuve de travail : type de mécanisme de consensus permettant de valider un enregistrement. Selon ce procédé, des mineurs (par opposition aux validateurs dans le cadre de la preuve par l'enjeu) rivalisent pour résoudre un problème cryptographique. Le mineur doit notamment prouver au réseau qu'il a effectué le chiffrement et, une fois la preuve apportée, l'enregistrement est ajouté au registre distribué. En principe, le mineur recevra des actifs numériques en récompense.

Preuve par l'enjeu : type de mécanisme de consensus permettant de valider un enregistrement. Selon ce procédé, des validateurs sont sélectionnés au hasard après avoir mis en jeu une certaine quantité d'actifs numériques. Lorsqu'un nombre précis de validateurs ont été sélectionnés et que ceux-ci confirment l'exactitude des données enregistrées, celles-ci sont intégrées au registre distribué.

Preuves à divulgation nulle de connaissance : méthode permettant à une partie de prouver à une autre partie qu'une proposition donnée est vraie sans communiquer d'autre information que le fait que la proposition est effectivement vraie.

Pseudonymat : utilisation d'adresses pseudonymes, qui sont des chaînes de caractères uniques générées par un processus cryptographique et servant à représenter des personnes dans les systèmes de registres distribués. Les adresses pseudonymes peuvent être reliées à une personne physique ou morale et ne garantissent donc pas l'anonymat.

Silo de données : ensemble de données qui sont normalement isolées de certains groupes d'utilisateurs et qui ne sont pas facilement accessibles à ces derniers.

Taux de hachage du minage : unité de mesure de la puissance de calcul nécessaire à un mineur pour résoudre un problème cryptographique donné.