

La chaîne de blocs peut-elle révolutionner le commerce international ?



Par Emmanuelle Ganne

La chaîne de blocs peut-elle révolutionner le commerce international ?

Par Emmanuelle Ganne



ORGANISATION
MONDIALE
DU COMMERCE

Avertissement

Les opinions exprimées dans cette étude sont celles de l'auteur. Elles ne sont pas censées représenter la position ou les points de vue de l'OMC ou de ses Membres, et elles sont sans préjudice des droits et des obligations des Membres dans le cadre de l'OMC. Son auteur est seul responsable en cas d'erreur.

© Organisation mondiale du commerce 2019

La reproduction d'informations contenues dans le présent document n'est possible qu'avec l'autorisation écrite du Responsable des publications de l'OMC.

ISBN (version imprimée): 978-92-870-4762-5

ISBN (version électronique): 978-92-870-4763-2

Publications de l'OMC

Organisation mondiale du commerce

154, rue de Lausanne

CH 1211 Genève 2

Suisse

Tél.: +41 (0)22 739 51 11

www.wto.org/fr

Courriel: publications@wto.org

Librairie en ligne de l'OMC: <http://onlinebookshop.wto.org>

Rapport conçu par Services Concept.

Imprimé par l'Organisation mondiale du commerce.

Crédits photo:

Couverture: © Getty/Photographer is my life.

Page 91: © Provenance.

Publié par l'Organisation mondiale du commerce.

Table des matières

<i>Remerciements</i>	<i>v</i>
<i>Résumé analytique</i>	<i>vii</i>
1. Introduction	1
2. La chaîne de blocs en bref	3
1. Petit historique	3
2. Chaîne de blocs 101	6
3. Types de chaînes de blocs	8
4. Les contrats intelligents : une invention intelligente sans composante intelligente	14
5. Des applications multiples... mais pas une solution pour tout	15
3. La chaîne de blocs peut-elle révolutionner le commerce international ?	19
1. Vers un commerce sans papier ?	19
2. Une nouvelle génération de services ?	52
3. Renforcement des droits de propriété intellectuelle	65
4. Amélioration des procédures de passation des marchés publics	77
4. Un monde de possibilités... et de défis	89
1. Des possibilités multiples	89
2. Le succès n'est pas acquis	104
5. Conclusion	127
Annexe – La chaîne de blocs pour les fans de technologie	129
Glossaire	137
Bibliographie	146
Abréviations	160
Liste des graphiques et tableaux	162

Remerciements

Mes sincères remerciements vont à ma collègue Kenza Le Mentec pour ses précieux conseils. Mme Le Mentec m'a initiée au sujet et elle a apporté de précieuses contributions, en particulier pour les sections techniques décrivant la technologie et pour la section sur la facilitation des échanges. Cette publication n'aurait pas été possible sans son soutien.

Je suis également très reconnaissante à Shashank Rai, spécialiste principal de la technologie stratégique au CIC, pour ses explications techniques et ses conseils et pour avoir pris le temps d'échanger des vues et de relire le rapport. Ses contributions techniques ont été extrêmement précieuses.

Mes remerciements vont aussi aux différents experts d'Accenture, de Deloitte, des douanes danoises et néerlandaises, d'Everledger, d'IBM, de Maersk, de VCargoCloud et de We.trade, qui ont pris le temps de discuter avec moi et de partager leurs idées sur la chaîne de blocs et les différents projets auxquels ils ont participé.

En outre, je tiens à remercier Enrico Camerinelli, analyste principal chez Aite Group, Shantanu Godbole, d'IBM Research, Philippe Heeren, avocat chez Deloitte Legal, Jonathan Koh, Directeur général de Trade Facilitation Pte Ltd, Lance Thompson, Secrétaire du CEFAC-T-ONU, CEE, ainsi que l'équipe d'Hyperledger, en particulier Brian Behlendorf, Directeur exécutif du projet Hyperledger, Ry Jones, architecte de communauté, et Marta Piekarska, Directrice d'Ecosystem, pour leurs observations d'ordre technique.

Je remercie également mes collègues de l'OMC qui m'ont fait part de leurs commentaires : Rob Anderson, Marc Auboin, Robert Koopman, Juan Marchetti, Nora Neufeld, Simon Padilla, Roberta Piermartini, Melvin Spreij, Jayashree Watal et Christiane Wolff.

Résumé analytique

La chaîne de blocs va bien au-delà du Bitcoin.

La première application de la chaîne de blocs comme support du bitcoin a amené à assimiler la chaîne de blocs au bitcoin. Cependant, son utilisation potentielle va bien au-delà du monde des cryptomonnaies. Pour certains, cette technologie va transformer nos vies, tandis que pour d'autres, c'est une chimère; aucune technologie n'a suscité autant de débats depuis l'avènement d'Internet. Pourtant, malgré les nombreux articles sur la chaîne de blocs, cette technologie reste difficile à appréhender pour beaucoup.

La chaîne de blocs: un registre de transactions numériques sécurisé, décentralisé et distribué qui inspire confiance et qui est réputé très résistant.

Une chaîne de blocs est un ensemble ou «registre» décentralisé et distribué de transactions qui y sont stockées de manière permanente et quasi inaltérable au moyen de techniques cryptographiques*.¹ À la différence des bases de données traditionnelles, qui sont administrées par une entité centrale, la chaîne de blocs repose sur un réseau pair à pair qu'aucune partie ne peut contrôler à elle seule. L'authentification des transactions s'effectue par des moyens cryptographiques et par un «protocole de consensus»* mathématique qui détermine les règles de mise à jour du registre, ce qui permet aux intervenants qui ne se font pas particulièrement confiance de collaborer sans qu'il soit besoin de recourir à un seul tiers de confiance. C'est pourquoi la chaîne de blocs est une «machine à créer de la confiance», comme la surnomme *The Economist*. Les participants à une chaîne de blocs peuvent accéder au registre et le vérifier à tout moment.

La chaîne de blocs garantit donc une transparence immédiate et absolue, et comme les transactions qui y sont ajoutées sont horodatées* et ne peuvent pas être facilement falsifiées, cette technologie permet de suivre facilement les produits et les transactions. Pour automatiser les processus et réduire davantage les coûts, il est possible d'utiliser des contrats intelligents*, c'est-à-dire des programmes

informatiques qui s'exécutent automatiquement quand certaines conditions sont remplies. En raison de leur nature décentralisée et distribuée et de l'utilisation de techniques cryptographiques, on considère que les chaînes de blocs résistent beaucoup mieux aux cyberattaques que les bases de données traditionnelles, même s'il n'existe pas de résistance parfaite.

Les chaînes de blocs peuvent être publiques, privées ou gérées par un consortium de sociétés, et elles peuvent être accessibles à tous (sans permission) ou restreintes (accessibles avec permission).

Une chaîne de blocs peut être catégorisée de diverses manières. Elle peut être publique (aucune entité spécifique ne gère la plate-forme), privée (la plate-forme est contrôlée par une seule entité) ou gérée par un consortium de sociétés. Une autre classification courante fait une distinction entre les chaînes de blocs accessibles sans permission (la chaîne de blocs est ouverte à tous, l'exemple le plus connu étant la plate-forme bitcoin) ou accessibles uniquement avec une permission (il peut y avoir des restrictions concernant les personnes qui peuvent lire et/ou écrire dans la chaîne de blocs). Dans la pratique, il existe de nombreuses variantes des chaînes de blocs, en fonction des objectifs visés. Dans le domaine du commerce international, beaucoup d'applications entrent dans la catégorie des chaînes accessibles avec permission/gérées par un consortium. Bien qu'à proprement parler, la chaîne de blocs ne soit qu'un type de technologie de registres distribués, l'expression est désormais couramment employée pour désigner plus généralement la technologie des registres.

Les applications commerciales potentielles de la chaîne de blocs sont nombreuses et pourraient profondément transformer le commerce international mais la technologie n'est pas une solution à tout.

Que ce soit la finance, y compris le financement du commerce, les formalités douanières, les processus de certification, le transport et la logistique, les assurances, la distribution, la propriété intellectuelle ou les marchés publics, les applications possibles de la chaîne de blocs comprennent différents domaines liés aux activités de l'OMC. Bien que cette technologie offre des possibilités intéressantes de renforcer l'efficacité d'un certain nombre de processus et de réduire les coûts dans ces domaines, ce n'est pas une panacée. Il est essentiel de peser soigneusement les coûts et les avantages.

La chaîne de blocs pourrait offrir de nouvelles possibilités de renforcer l'efficacité des processus dans un certain nombre de domaines liés aux activités de l'OMC.

La chaîne de blocs pourrait contribuer à la dématérialisation accrue du commerce.

Qu'il s'agisse de financement du commerce, de dédouanement, de transport ou de logistique, le commerce des marchandises fait intervenir de multiples acteurs et nécessite encore beaucoup de papier. Nombreux sont ceux qui considèrent la chaîne de blocs comme un moyen intéressant d'améliorer l'efficacité des processus commerciaux et de progresser vers un commerce sans papier. Cependant, les défis à relever sont du même ordre de grandeur que les possibilités offertes par la technologie.

On considère que la chaîne de blocs pourrait changer la donne en permettant de numériser et d'automatiser les processus de financement du commerce, en particulier les lettres de crédit, et de faciliter le financement des chaînes d'approvisionnement. Un grand nombre de banques travaillant avec des startups de technologie financière (fintech) et des sociétés de technologie de l'information étudient le potentiel de la chaîne de blocs. Les projets pilotes sont encourageants, mais un certain nombre de questions techniques et réglementaires doivent être réglées avant que cette technologie puisse être utilisée à grande échelle.

Les caractéristiques intrinsèques de la chaîne de blocs en font un outil potentiellement intéressant pour aider à mettre en œuvre l'Accord de l'OMC sur la facilitation des échanges (AFE) et faciliter les processus entre entreprises et gouvernements (B2G) et entre gouvernements (G2G) au niveau national. La chaîne de blocs et les contrats intelligents pourraient aider à administrer les procédures aux frontières et les guichets uniques nationaux (point d'entrée unique par lequel les acteurs du commerce peuvent présenter des documents et d'autres renseignements pour accomplir les formalités douanières) d'une manière plus efficace, plus transparente et plus sûre, et à améliorer l'exactitude des données commerciales. Le véritable défi sera d'accroître l'efficacité des processus G2G transfrontaliers. Pour ce faire, il ne faudra pas seulement régler les problèmes d'interopérabilité au niveau technique – question sur laquelle la communauté de la chaîne de blocs travaille activement –, mais il faudra aussi assurer la normalisation et faire preuve de volonté politique pour créer un cadre réglementaire propice au commerce sans papier.

Enfin, cette technologie ne pourra fonctionner à son plein potentiel que si tous les aspects des transactions commerciales transfrontières sont numérisés, du

financement du commerce aux formalités douanières, au transport et à la logistique, et si la sémantique est alignée (c'est-à-dire si l'on sait quels renseignements sont communiqués par les éléments de données). Dans le secteur du transport et de la logistique, terrain fertile pour l'application de la chaîne de blocs en raison du grand nombre d'acteurs impliqués, on étudie activement les moyens de tirer parti de cette technologie pour développer des plates-formes commerciales qui pourraient relier tous les acteurs de la chaîne logistique, y compris les banques et les autorités douanières.

Si les projets en cours de développement aboutissent, la chaîne de blocs pourrait bien être l'avenir de l'infrastructure commerciale et le plus grand disrupteur du secteur du transport maritime et du commerce international depuis l'invention du conteneur. Mais, il reste beaucoup à faire. De tels projets nécessitent un travail d'intégration complexe et un cadre réglementaire favorable. De plus, ils posent des problèmes d'interopérabilité et de normalisation. Un dialogue entre toutes les parties prenantes, y compris les régulateurs, est essentiel.

La chaîne de blocs pourrait donner naissance à une nouvelle génération de services.

Outre les projets pilotes de chaîne de blocs axés sur le financement du commerce, un nombre croissant de startups développent des produits et des applications de chaînes de blocs pour accélérer et faciliter les paiements transfrontières et en réduire le coût, ce qui pousse les établissements financiers bien établis à repenser leur façon de faire.

Toutefois, il est peu probable que le paysage financier change radicalement. Ironiquement, la chaîne de blocs pourrait même servir à renforcer les établissements financiers que « Satoshi Nakamoto », pseudonyme du ou des fondateurs de la chaîne de blocs, voulait rendre superflus.

La technologie de la chaîne de blocs pourrait aussi avoir un impact considérable sur un autre secteur, celui des assurances. L'automatisation des processus grâce à l'utilisation de contrats intelligents pourrait aider à alléger les procédures administratives, à réduire leurs coûts, à traiter les demandes de remboursement et à gérer les contrats d'assurance multinationaux. Les projets pilotes testés dans le secteur des assurances maritimes présentent un intérêt particulier pour le commerce international.

La chaîne de blocs commence aussi tout juste à faire son entrée dans le monde du commerce électronique. Elle ne va peut-être pas révolutionner le commerce électronique en soi, mais elle pourrait lui donner une nouvelle impulsion et avoir une incidence sur les modèles économiques existants.

Si les initiatives en cours sont concluantes et si les questions techniques et juridiques sont résolues, la chaîne de blocs pourrait devenir la future « infrastructure » du secteur des services. En raison de ses capacités d'automatisation et grâce à l'utilisation de contrats intelligents, la chaîne de blocs pourrait être au secteur des services ce que les robots ont été au secteur manufacturier. Toutefois, il est peu probable que les relations au sein d'un secteur en soient bouleversées. Le principal effet de la chaîne de blocs se fera très probablement sentir en termes de réduction des coûts.

La chaîne de blocs pourrait aider à administrer les droits de propriété intellectuelle de manière plus efficiente et plus transparente et contribuer à la lutte contre la contrefaçon.

Dans de nombreux pays, de plus en plus d'entreprises examinent comment la technologie de la chaîne de blocs peut être utilisée pour améliorer l'administration et le respect des droits de propriété intellectuelle (DPI). Les applications de la chaîne de blocs dans ce domaine sont nombreuses et pourraient avoir une incidence à la fois sur la gouvernance des droits de propriété intellectuelle et sur le secteur de la propriété intellectuelle lui-même. Pour les droits enregistrés ou non enregistrés, la chaîne de blocs pourrait sans doute être utilisée pour apporter la preuve de la création, de l'existence, de la propriété et/ou de la première utilisation, pour enregistrer les DPI, pour faciliter leur administration et leur gestion à l'échelle mondiale, ce qui pourrait contribuer à l'émergence de « chaînes mondiales de propriété intellectuelle », et pour faire respecter les DPI et lutter plus efficacement contre la contrefaçon.

Bien que les applications de la technologie de la chaîne de blocs puissent permettre de remédier à certains des problèmes rencontrés par les titulaires de droits, cette technologie ne résoudra pas tout. Mais une chose est sûre : son caractère disruptif, la multiplicité des applications potentielles et leurs implications pratiques et juridiques méritent l'attention des régulateurs et des législateurs.

La chaîne de blocs pourrait améliorer les processus de passation des marchés publics, mais il faut sopeser attentivement les coûts et les avantages.

La chaîne de blocs promet d'améliorer les processus de passation des marchés publics, de renforcer l'efficacité de la gestion des marchés publics et de contribuer à la lutte contre la fraude, mais il reste à voir si les preuves de concept (ou démonstrations de faisabilité) actuelles sont concluantes et si l'utilisation de la chaîne de blocs peut permettre de sécuriser et d'automatiser davantage les systèmes de passation des marchés en ligne, et ce à un coût qui justifie le passage à un système fondé sur cette technologie.

Au-delà des applications sectorielles spécifiques, la chaîne de blocs offre des possibilités transversales très diverses. Elle pourrait aider à renforcer la confiance et à accroître la transparence des chaînes d'approvisionnement.

Comme elle offre de nouveaux moyens de suivre le parcours des produits, la chaîne de blocs peut être un puissant moyen de promouvoir la transparence et la traçabilité des chaînes d'approvisionnement, de contribuer à la lutte contre la contrefaçon et de renforcer la confiance des consommateurs. Beaucoup de start-up et d'entreprises bien établies développent des applications de chaînes de blocs permettant de retracer l'origine des produits, de prouver leur authenticité et leur qualité et de faire valoir des allégations éthiques et des pratiques commerciales équitables. À la suite des différents scandales qui ont secoué l'industrie alimentaire ces dernières années, les grandes entreprises de l'agroalimentaire et de la distribution se tournent vers la chaîne de blocs, non seulement pour améliorer la transparence de la chaîne d'approvisionnement alimentaire, mais aussi pour pouvoir localiser rapidement les produits contaminés et restaurer la confiance des consommateurs dans la qualité des aliments. Toutefois, il est essentiel d'établir un lien crédible entre ce qui se passe en ligne et hors ligne, et cela peut s'avérer coûteux. En effet, la qualité des informations ajoutées à la chaîne de blocs dépend de la fiabilité du processus de vérification hors ligne qui garantit que les exigences pertinentes ont été respectées hors ligne.

La chaîne de blocs peut réduire considérablement les coûts du commerce.

En renforçant la transparence et en permettant d'automatiser les processus et les paiements, la chaîne de blocs pourrait réduire considérablement les coûts du

commerce, notamment les coûts de vérification, de mise en réseau, de traitement, de coordination, de transport et de logistique, ainsi que les coûts d'intermédiation financière et les frais de change. Bien qu'il soit difficile d'évaluer dans quelle mesure le déploiement de la technologie de la chaîne de blocs aura un effet sur les coûts du commerce, il semble à première vue que celui-ci sera considérable. On estime que la réduction des coûts dans le secteur financier et le secteur du transport maritime représentera entre 15 et 30% des coûts totaux. Selon le Forum économique mondial, l'élimination des obstacles grâce à la chaîne de blocs pourrait entraîner une augmentation du commerce de plus de 1 000 milliards de dollars au cours de la prochaine décennie.

La chaîne de blocs ouvre de nouvelles possibilités aux micro, petites et moyennes entreprises (MPME) et aux petits producteurs des pays en développement.

La chaîne de blocs pourrait être un puissant moyen de promouvoir la participation des MPME au commerce international en facilitant l'accès au financement du commerce, en simplifiant les procédures commerciales et en réduisant les coûts du commerce. Elle pourrait permettre de réduire les obstacles à l'entrée de sorte que les petites entreprises et les petits producteurs pourraient participer plus facilement au commerce international.

Toutefois, ces possibilités ne peuvent se concrétiser que si les petites entreprises et les petits producteurs disposent des compétences techniques nécessaires et d'un bon accès à Internet. Il est donc essentiel de combler le fossé numérique, à la fois en termes d'accès et de bande passante. De plus, comme toute innovation, la chaîne de blocs risque d'avoir un effet disruptif sur certains secteurs et sur certaines catégories de travailleurs. Il se peut que les possibilités et les bénéfices ne soient pas également répartis.

Cependant, ces possibilités ne se concrétiseront que si plusieurs grands problèmes sont résolus, notamment les problèmes techniques comme la scalabilité...

De nombreux observateurs soulignent la scalabilité limitée de la chaîne de blocs due à la taille prédéterminée des blocs et aux problèmes de consommation d'énergie. Si la question de la scalabilité est particulièrement pertinente pour les chaînes de blocs publiques, elle l'est moins pour les chaînes de blocs soumises à l'autorisation d'un consortium, qui ne font pas l'objet des mêmes limitations. Ces dernières, qui ont un grand potentiel pour le commerce international, ont une plus

grande scalabilité. La vive controverse au sujet de la consommation d'énergie des chaînes de blocs concerne surtout les chaînes accessibles sans permission. En outre, de nouveaux algorithmes sont actuellement développés – dont beaucoup s'éloignent du concept de blocs –, qui sont plus rapides et moins gourmands en énergie et qui sont donc plus «scalables».

Un autre problème technique qui pourrait se poser à long terme concerne les questions de sécurité. Bien que les chaînes de blocs soient très résistantes par rapport aux bases de données traditionnelles en raison de leur caractère décentralisé et distribué et de l'utilisation de techniques de cryptographie, elles ne sont pas totalement à l'abri des problèmes de sécurité classiques, et les progrès des technologies, en particulier de l'informatique quantique, pourraient, à long terme, représenter une menace pour la technologie de la chaîne de blocs. Les algorithmes «post-quantiques», résistants à l'informatique quantique, font l'objet de recherches intenses.

... l'interopérabilité, ...

L'un des principaux défis concernant la chaîne de blocs est celui de l'interopérabilité, tant au niveau technique qu'au niveau sémantique (c'est-à-dire quelle information est communiquée par l'élément de données). De nombreuses plates-formes sont actuellement développées qui utilisent des interfaces techniques et des algorithmes différents et qui ne «communiquent pas entre elles». Ce problème de «l'îlot numérique» fait l'objet de recherches actives au sein de la communauté des chaînes de blocs. Des solutions techniques émergent, mais elles n'en sont encore qu'à leurs balbutiements.

La sémantique de l'information échangée est aussi examinée de près pour s'assurer que l'expéditeur, le destinataire et tout utilisateur qui consulte l'information comprennent les données de la même manière. Des organisations internationales telles que la Chambre de commerce internationale (ICC), l'Organisation internationale de normalisation (ISO), le Centre des Nations Unies pour la facilitation du commerce et les transactions électroniques (CEFACT-ONU) et l'Organisation mondiale des douanes (OMD) ont créé des groupes de travail pour engager des discussions sur la question et élaborer des normes d'interopérabilité.

... et les questions juridiques.

Le déploiement de la chaîne de blocs à grande échelle nécessite un cadre réglementaire favorable qui reconnaît la validité juridique des transactions gérées

par des chaînes de blocs, précise la loi applicable et les responsabilités et réglemente la manière dont les données peuvent être consultées et utilisées. La question la plus importante est celle du statut juridique des transactions gérées par des chaînes de blocs. Il faut que la législation reconnaisse la validité des signatures électroniques, des documents électroniques et des transactions électroniques, en particulier des transactions gérées par des chaînes de blocs. En 2017, la Commission des Nations Unies pour le droit commercial international (CNUDCI) a adopté la loi type sur les documents transférables électroniques, et plusieurs gouvernements travaillent à l'élaboration d'une loi reconnaissant les transactions gérées par des chaînes de blocs, mais beaucoup reste à faire. Quant aux questions relatives au droit applicable et à la responsabilité, qui sont problématiques dans le cas des chaînes de blocs sans permission, des solutions techniques peuvent souvent être trouvées lorsqu'il s'agit des chaînes de blocs avec permission.

La question juridique de la confidentialité des données et du droit à l'oubli inscrits dans certaines législations peut aussi poser problème. Le principe de la chaîne de blocs et celui du droit à l'oubli semblent a priori incompatibles. Certains observateurs soulignent toutefois que les deux visent le même objectif, à savoir donner aux individus davantage de contrôle sur leurs données personnelles, mais au moyen de mécanismes différents.

Enfin, deux questions juridiques pourraient faciliter l'application de la technologie de la chaîne de blocs : la codification du droit, qui vise à rendre les lois lisibles par machine afin de faciliter la transposition des obligations contractuelles dans un code de contrat numérique (contrat intelligent), et le développement d'une identification juridique mondiale des entreprises.

Étant donné l'impact considérable que la chaîne de blocs pourrait avoir sur le commerce mondial, il est essentiel de comprendre les implications juridiques de cette technologie et de développer des solutions collectives qui permettent de déployer cette technologie tout en répondant aux préoccupations juridiques.

Pour soutenir le déploiement à grande échelle de cette technologie, il est essentiel de mettre en place un écosystème complet calqué sur l'approche de la gouvernance d'Internet, qui réunit des entreprises, des organisations de la société civile, des développeurs de logiciels, des universitaires, des gouvernements et des organisations intergouvernementales dans différents cadres pour examiner les questions de normalisation et les questions juridiques et politiques.

De même, il serait utile d'examiner s'il faut engager une discussion sur les implications pratiques et juridiques de la chaîne de blocs dans les organisations internationales pertinentes telles que l'OMC, afin de mettre en lumière les bénéfices

potentiels de cette technologie, ses limites et les problèmes qui peuvent se poser si elle est déployée à plus grande échelle, et de trouver des solutions collectives pour soutenir l'utilisation d'une technologie qui pourrait avoir un impact considérable sur le commerce mondial.

La chaîne de blocs pourrait rendre le commerce international plus intelligent, mais un commerce intelligent exige des solutions et une normalisation intelligentes, qui ne peuvent être développées que par la coopération. Si l'on parvient à créer un écosystème propice au développement plus large de la chaîne de blocs, le commerce international pourrait être radicalement différent dans 10 ou 15 ans.

Notes de fin

1. Les termes ou expressions marqués d'un astérisque (*) sont définis dans le glossaire.

Principales caractéristiques de la chaîne de blocs

- **Une architecture de confiance décentralisée, distribuée et transparente:** Les informations ajoutées à la chaîne de blocs sont immédiatement visibles par tous les membres du réseau et elles sont distribuées, c'est-à-dire que chaque pair conserve une copie complète des données (ou une copie aussi proche que possible), et les mises à jour éventuelles sont partagées avec l'ensemble du réseau sans passer par une tierce partie centralisée. La chaîne de blocs assure une transparence immédiate et générale, bien que, dans le cas des chaînes de blocs avec permission (voir la section 2.3), la confiance soit plus centralisée et la lisibilité de certaines informations puisse être limitée aux participants ayant une permission, afin de mieux répondre aux objectifs de la chaîne de blocs.
- **Haute sécurité, immuabilité et traçabilité:** L'utilisation concomitante de diverses techniques cryptographiques et le caractère décentralisé et distribué des plates-formes de la chaîne de blocs font qu'elle est très résistante aux attaques par rapport aux bases de données traditionnelles. Cependant, bien que la technologie elle-même assure un haut niveau de sécurité, il subsiste des faiblesses liées aux contrats intelligents, aux interfaces utilisateurs et aux clés privées utilisées pour le cryptage, qui peuvent être volées au moyen d'attaques conventionnelles si elles sont enregistrées sur l'ordinateur d'un utilisateur ou un serveur centralisé.¹

L'information ajoutée à la chaîne de blocs est horodatée et ne peut pas être aisément modifiée. Cela a plusieurs conséquences :

- Premièrement, il est facile de détecter les tentatives de modification. Cela est particulièrement important dans un monde où les objets numériques peuvent être copiés, modifiés et partagés pour ainsi dire gratuitement. L'immutabilité de la chaîne de blocs permet d'authentifier facilement les produits et les documents. Il faut cependant noter que si la chaîne de blocs peut permettre d'empêcher les fraudes sur le registre, son inviolabilité n'empêche pas l'introduction de fausses informations dans le registre.
- Deuxièmement, en raison du caractère immuable et distribué de la chaîne de blocs, il n'est plus nécessaire de sauvegarder les bases de données, ce qui change fondamentalement la reprise après sinistre. Une fois ajoutées à la chaîne de blocs, les informations sont partagées avec

l'ensemble du réseau et enregistrées sur tous les nœuds, et il est pratiquement impossible de les modifier. Si un nœud est affecté par un sinistre, l'information peut facilement être récupérée.

- **Automatisation :** L'utilisation de contrats intelligents, c'est-à-dire de programmes informatiques qui s'exécutent automatiquement, permet d'automatiser les processus et les paiements, entre autres, ce qui accroît l'efficacité.

Note de fin

1. S'il connaît la clé privée, l'attaquant peut transférer des avoirs du compte du titulaire légitime de la clé privée à son propre compte. Dans le cas de la chaîne de blocs, l'absence d'entité centralisée signifie que la transaction ne peut pas être annulée. Le piratage d'entités centralisées dans les réseaux Bitcoin et Ethereum ont entraîné des pertes massives, mais il existe des moyens techniques qui permettent aux utilisateurs d'empêcher le vol de clés privées, comme les portefeuilles matériels, type spécial de portefeuille qui stocke les clés privées de l'utilisateur dans un dispositif matériel sécurisé.

1 Introduction

Le monde est en constante évolution, porté par les innovations technologiques qui influent sur notre façon de vivre et de faire des affaires. L'histoire de l'économie mondiale est intimement liée aux progrès technologiques. L'invention de la machine à vapeur a conduit à la mécanisation de la production, la découverte de l'électricité a permis la production de masse et, grâce à l'essor d'Internet, il est devenu possible de coordonner à distance les différentes étapes de la production, ce qui a entraîné la fragmentation de la production et l'apparition des chaînes de valeur mondiales.

Cependant, si les technologies de l'information et de la communication ont profondément transformé l'organisation de la production, elles n'ont pas encore permis de numériser les opérations commerciales. Malgré les efforts faits récemment pour mettre en place des processus électroniques afin de faciliter certains aspects des procédures commerciales, tels que les guichets uniques électroniques, les transactions commerciales dépendent encore beaucoup du papier. L'expédition de roses du Kenya à Rotterdam peut générer une pile de papier de 25 cm de haut, dont le coût de traitement peut être supérieur au coût du transport des conteneurs (Allison, 2016).

Les efforts pour numériser le commerce ont été entravés par les préoccupations en matière de sécurité et par la difficulté de coordonner les flux de données à travers les frontières et entre les multiples parties impliquées dans une transaction commerciale internationale. Une nouvelle technologie, la chaîne de blocs, est considérée par beaucoup comme une technologie pouvant changer la donne. Mais en quoi consiste la chaîne de blocs et quel est le potentiel de cette technologie pour le commerce international ?

Une chaîne de blocs est un registre numérique de transactions, qui est décentralisé (aucune entité ne contrôle seule le réseau), qui est distribué (les dossiers sont partagés avec tous les participants) et dans lequel les transactions sont stockées de manière très sûre, vérifiable et permanente au moyen de diverses techniques cryptographiques*. Les transactions enregistrées, dont le nombre augmente continuellement, sont combinées en «blocs» qui sont «enchaînés» les uns aux autres au moyen de la cryptographie, d'où l'expression «chaîne de blocs». Étant donné que les transactions sont partagées, vérifiées et validées de pair à pair, la chaîne de blocs peut fonctionner sans qu'il soit nécessaire de recourir à une autorité centrale ou un tiers de confiance, et l'information, une fois ajoutée à une chaîne de

blocs, est horodatée* et difficile à modifier. La chaîne de blocs permet donc de créer un registre partagé et fiable que tous les participants peuvent consulter et vérifier à tout moment, mais qu'aucune partie ne peut contrôler seule. C'est une « machine de confiance », comme l'a surnommée *The Economist* (2015). En raison de l'utilisation de diverses techniques cryptographiques et de son caractère décentralisé et distribué, la chaîne de blocs est censée être très résistante.

Développée à l'origine comme la technologie sous-jacente d'une cryptomonnaie, le bitcoin, les applications de la chaîne de blocs se sont rapidement répandues dans d'autres domaines. Du fait de son caractère transparent, sûr et immuable, la chaîne de blocs a suscité l'intérêt du secteur privé et des autorités publiques. Le nombre de preuves de concept et de projets pilotes augmente rapidement, et les applications touchent tous les secteurs de l'économie et de la société, de la finance au commerce électronique, de la sécurité sanitaire des aliments à la gestion des chaînes d'approvisionnement et même au vote, de nombreuses applications étant des chaînes de blocs « avec permission », c'est-à-dire qu'une autorisation est nécessaire pour effectuer des transactions dans le registre. Des milliards de dollars sont investis dans les sociétés de chaînes de blocs, et le nombre de brevets liés à cette technologie est en augmentation. En 2017, le financement par capital-risque des startups de chaînes de blocs n'a cessé de croître pour atteindre 1 milliard de dollars (CB Insights, 2018), et le nombre de demandes de brevets liés à la chaîne de blocs a triplé (Noonan, 2018). Cet engouement est-il justifié ?

Une innovation qui change la donne, une révolution, un énorme potentiel inexploité, la solution à tous les problèmes, un remède miracle pour certains ; du neuf avec du vieux, un jeu à somme nulle, beaucoup de bruit pour rien, une solution qui cherche un problème, une chimère et une technologie surestimée pour d'autres. La liste des qualificatifs hyperboliques apparaissant dans la littérature sur les chaînes de blocs est longue. Aucune technologie n'a suscité autant de passion populaire depuis l'avènement d'Internet, et aucune n'a provoqué autant de controverses en dehors du monde mystérieux des spécialistes des technologies de l'information (TI). Tout le monde a une opinion, mais rares sont ceux qui comprennent vraiment de quoi il s'agit.

La présente publication tente de démythifier le phénomène de la chaîne de blocs en expliquant de manière simple en quoi consiste cette technologie et quelles sont ses principales fonctionnalités.¹ Elle présente certaines applications liées au commerce et analyse la pertinence de cette technologie pour le commerce international en examinant comment elle est utilisée ou peut être utilisée dans les différents domaines couverts par l'OMC. Elle se demande si l'adoption généralisée de cette technologie pourrait avoir une incidence sur les transactions commerciales transfrontières et dans l'affirmative, dans quelle mesure, et elle examine les différents défis à relever pour qu'elle puisse être utilisée à grande échelle.²

Note de fin

1. La présente étude porte sur la technologie elle-même, et non sur les cryptomonnaies.
2. Les informations données dans cette publication sont valables à compter de septembre 2018.

2 La chaîne de blocs en bref

1. Petit historique

La chaîne de blocs est une technologie qui a vu le jour en 2008 dans la communauté des experts en cryptographie*.¹ Elle a été conceptualisée par un individu ou un groupe d'individus non encore identifiés utilisant le pseudonyme de Satoshi Nakamoto. Elle a été appliquée pour la première fois en 2009 comme fondement de la cryptomonnaie bitcoin.² Bien que la chaîne de blocs et le bitcoin soient historiquement liés, ce sont deux choses distinctes. La chaîne de blocs est la technologie qui sous-tend le bitcoin ; c'est l'infrastructure virtuelle sur laquelle il repose. Le bitcoin est une cryptomonnaie, mais le terme est souvent utilisé pour désigner à la fois la cryptomonnaie et le protocole qui la sous-tend, c'est-à-dire la chaîne de blocs. Cette confusion est peut-être une des raisons pour lesquelles le public a mis tant de temps à réaliser que la chaîne de blocs peut être utilisée dans des domaines autres que les cryptomonnaies.

Le bitcoin ayant été lancé au lendemain de la crise financière de 2008, il a été considéré à tort comme une conséquence directe de la crise. Mais l'histoire des cryptomonnaies a en fait commencé avant la crise.

Plusieurs cryptomonnaies plus anciennes n'ont pas réussi à décoller et ne sont jamais sorties de la communauté de la cryptographie. Les ancêtres du bitcoin ont été créés par les membres des «Cypherpunks», réseau d'activistes préconisant l'utilisation généralisée d'une cryptographie robuste et de technologies améliorant la protection de la vie privée comme moyen de changement social et politique. Les Cypherpunks utilisaient les systèmes de pair à pair et la cryptographie pour traiter les transactions de manière sécurisée sans élément «Big Brother», expression par laquelle ils désignaient le système bancaire.

La crise financière de 2008 a ouvert la voie à l'opérationnalisation, à l'adoption et à l'expansion des cryptomonnaies, en particulier du bitcoin (Bustillos, 2013). Du fait de la perte de confiance dans la gouvernance du système monétaire et, par extension, dans la gouvernance publique en général, certains ont vu dans le bitcoin une solution de remplacement souhaitable, la réalisation de tous les idéaux

défendus par les Cypherpunks. Dans son livre blanc de 2008, «Bitcoin : A Peer-to-Peer Electronic Cash System» (Nakamoto, 2008), Satoshi Nakamoto décrit un nouveau modèle de confidentialité, dans lequel le tiers de confiance entre les deux parties effectuant une transaction est remplacé par des preuves cryptographiques, fournies et validées par les pairs, évitant ainsi les points de défaillance uniques qui existent dans le modèle traditionnel de confidentialité (c'est-à-dire les banques dans les systèmes de monnaie fiduciaire³). Selon Satoshi Nakamoto, le nouveau modèle a résolu le problème de la «double dépense», c'est-à-dire le fait que les monnaies numériques peuvent être dépensées plus d'une fois parce que le fichier numérique peut être copié. En outre, ce nouveau système permettait de rendre les transactions publiques tout en conservant l'anonymat des parties concernées, ce qui améliorerait la transparence tout en protégeant la confidentialité. Enfin, le caractère immuable du bitcoin et l'horodatage* offraient des garanties importantes contre la fraude à un moment où les grands acteurs du système financier défrayaient la chronique pour avoir trafiqué les comptes et les indicateurs de marché.

Bien que le bitcoin ait été la première application concrète de la chaîne de blocs, cette technologie est en fait une combinaison de plusieurs techniques sous-jacentes qui existent depuis au moins quatre décennies. Pendant les cinq années qui ont suivi la création du bitcoin, l'histoire de la chaîne de blocs a été pratiquement synonyme de l'histoire du bitcoin. Ce n'est qu'à partir de 2013 que la technologie de la chaîne de blocs a commencé à se faire un nom du fait de son utilisation dans d'autres cryptomonnaies comme Ethereum (voir Investoo Group, 2017), et plus récemment en dehors du secteur des technologies financières (fintech).

La création d'Ethereum a marqué un deuxième tournant dans l'histoire de la chaîne de blocs. En 2013, un jeune programmeur de 19 ans, Vitalik Buterin a publié un livre blanc dans lequel il exposait son plan pour une chaîne de blocs qui faciliterait aussi les «applications décentralisées» (Buterin, 2013). Pour cela, il proposait d'intégrer dans Ethereum un langage de programmation que les développeurs pourraient adapter en fonction de leurs besoins.

Ethereum, parfois appelé la «chaîne de blocs 2.0», a été lancé à la fin de 2015. La plate-forme a fait un bond en avant avec le concept des contrats intelligents*, c'est-à-dire des programmes informatiques qui exécutent automatiquement les clauses d'un contrat lorsque certaines conditions sont remplies. Les applications des contrats intelligents fonctionnent exactement comme elles ont été programmées, sans fraude ni interférence de tiers ni retard. Cette automatisation des transactions a été une révolution dans la révolution et c'est l'une des caractéristiques les plus utiles de la chaîne de blocs pour le commerce.

Le moment probablement le plus marquant dans l'histoire de la chaîne de blocs a ensuite été l'attaque dirigée à la mi-2016 contre l'organisation autonome décentralisée⁴ (DAO) d'Ethereum. La DAO était censée fonctionner comme un fonds de capital-risque pour l'espace cryptographique et était conçue comme un contrat intelligent adossé à la chaîne de blocs d'Ethereum. Quelques semaines après son lancement, elle a fait l'objet d'une attaque informatique, qui a siphonné des millions de dollars d'actifs et entraîné l'effondrement de la DAO. Cela a amené de nombreux sceptiques à mettre en doute les fondements mêmes de la chaîne de blocs, à savoir son immuabilité et sa résistance aux attaques (voir aussi Siegel, 2016). Or le problème n'était pas la technologie elle-même, mais le codage des programmes de contrats qui alimentaient la DAO. Les programmes, qui avaient été construits sur le registre de la chaîne de blocs d'Ethereum, comportaient un défaut qui permettait, dans certaines circonstances, de vider les comptes bloqués⁵ (Brandon, 2016).

Malgré cet incident malheureux, les contrats intelligents sont l'une des caractéristiques de la chaîne de blocs qui suscitent aujourd'hui le plus d'intérêt pour des centaines d'applications dans tous les domaines en raison de leur souplesse et de la possibilité d'automatiser les processus.

Au cours des dernières années, un éventail de nouvelles technologies des registres distribués a été mis au point pour améliorer les capacités des réseaux Bitcoin et Ethereum et promouvoir de nouveaux cas d'utilisation⁶ (voir la section suivante pour plus de renseignements sur la relation entre la chaîne de blocs et la technologie des registres distribués). Par exemple, la technologie IOTA, qui est une technologie des registres distribués mais pas une chaîne de blocs en soi car elle ne combine pas les transactions dans des blocs et elle ne les enchaîne pas de manière linéaire, a été lancée en 2016 en tant que plate-forme de cryptomonnaie conçue pour la communication de machine à machine.⁷

En outre, divers consortiums ont été formés pour développer des solutions adaptées aux besoins des entreprises. Le consortium R3, par exemple, qui regroupe plus de 200 entreprises, régulateurs et associations professionnelles, a développé sa propre plate-forme de registres distribués appelée Corda, qui est orientée vers le monde financier.⁸

Une autre initiative très connue est Hyperledger, qui est hébergée par la Linux Foundation, organisation à but non lucratif réunissant des leaders des secteurs de la finance, des banques, de l'Internet des objets (dispositifs machine à machine), des chaînes d'approvisionnement, de l'industrie et de la technologie pour faire progresser les technologies de chaînes de blocs intersectorielles. Hyperledger est le fruit d'un effort de collaboration visant à développer des cadres d'utilisation pour entreprises

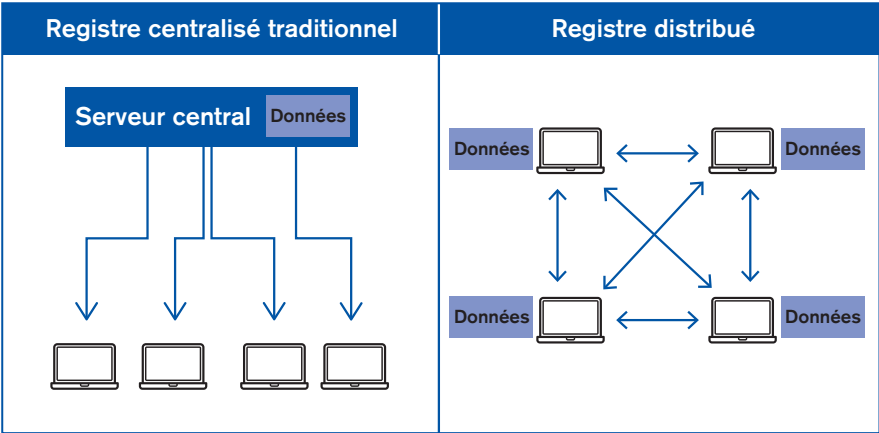
fondés sur la chaîne de blocs ainsi que des logiciels libres et des outils connexes. Hyperledger est maintenant largement utilisé dans divers domaines, y compris le commerce international.⁹

2. Chaîne de blocs 101

Une chaîne de blocs est un registre numérique de transactions, qui est décentralisé (aucune entité contrôle seule le réseau, bien qu'il existe des chaînes de blocs «privées», qui sont plus centralisées, voir la section 2.3), qui est distribué (les dossiers sont partagés avec tous les participants) et qui est sécurisé au moyen de plusieurs techniques cryptographiques éprouvées. Une chaîne de blocs est gérée par des ordinateurs ou des serveurs – appelés «nœuds»* – en pair à pair, sans qu'il soit nécessaire de passer par les intermédiaires qui authentifient habituellement les transactions (comme les banques dans le cas des transactions financières). Les données ajoutées à la chaîne de blocs sont partagées avec tous les membres du réseau et sont vérifiées et validées par n'importe quelle personne ayant les permissions appropriées sur la base du protocole de consensus* de la chaîne de blocs (voir la figure 1).

Les données ajoutées à la chaîne de blocs sont «hachées»*, c'est-à-dire qu'elles sont converties en une nouvelle chaîne numérique d'une longueur fixe au moyen d'une fonction mathématique, et qu'elles sont chiffrées* pour assurer leur intégrité, empêcher la falsification et garantir que le message a été créé et envoyé par l'expéditeur déclaré et n'a pas été modifié lors du transit. Si l'expéditeur de la

Figure 1 Registre centralisé et registre distribué



Source: Auteure.

transaction ne souhaite pas que les autres membres du réseau voient le contenu du message, c'est-à-dire les données en clair qui se trouvent dans les documents soumis, il peut choisir de chiffrer le message lui-même, rendant ainsi les données inintelligibles pour les personnes qui ne sont pas autorisées à y accéder.

Une fois validées, les transactions sont stockées dans des «blocs» qui sont «enchaînés» les uns aux autres par ordre chronologique au moyen de techniques cryptographiques (voir l'annexe pour une description d'une transaction de chaîne de blocs type).¹⁰ Les données, une fois ajoutées à une chaîne de blocs, sont horodatées*, et il est pratiquement impossible de les modifier. Toutefois, bien que la chaîne de blocs puisse aider à empêcher la fraude sur le registre, son inviolabilité ne peut pas empêcher l'introduction de fausses informations dans le registre.

Dans une chaîne de blocs, chaque pair conserve une copie complète des données (ou une version aussi proche que possible), et les mises à jour sont partagées avec tous les participants simultanément. Les participants à une chaîne de blocs ont donc tous accès aux mêmes informations à tout moment. En d'autres termes, une chaîne de blocs est un registre partagé et fiable que tous les participants peuvent consulter et vérifier à tout moment, mais qu'aucune partie ne peut contrôler seule (sauf s'il est entièrement privé, voir la section suivante), ce qui permet aux personnes qui ne se font pas particulièrement confiance de collaborer sans passer par des intermédiaires de confiance.

Étant donné que les données sont répliquées autant de fois qu'il y a de nœuds, la falsification des données ou la compromission de l'ensemble du réseau obligerait à compromettre un grand nombre de nœuds, ce qui serait difficile dans la pratique, mais pas impossible. En théorie, un réseau de chaîne de blocs peut être compromis si un validateur ou un groupe de validateurs contrôle plus de 50% de la puissance de calcul du réseau, ce qu'on appelle une «attaque à 51%». Bien que l'attaque à 51% soit un problème commun à tous les types de chaînes de blocs, elle est particulièrement dangereuse dans le cas des chaînes de blocs publiques, car il est difficile de déterminer qui valide effectivement les blocs.

Ce qui caractérise les chaînes de blocs publiques, c'est la puissance de calcul considérable dont la plupart ont besoin pour valider les transactions, en particulier celles qui utilisent le mécanisme de consensus basé sur la preuve de travail, comme le bitcoin (voir l'annexe pour plus de renseignements). Bien qu'elle gaspille beaucoup d'énergie, la preuve de travail est nécessaire pour assurer la sécurité du processus de consensus. Cela rend les chaînes de blocs publiques mathématiquement très difficiles à pirater, car le coût du piratage est trop élevé pour un système dont chaque nœud connecté est synchronisé avec l'ensemble du réseau de chaîne de blocs. Par conséquent, bien que le piratage du système ne soit pas impossible, il est

économiquement inefficent et extrêmement difficile dans la pratique. Cependant, la puissance de calcul est de plus en plus agrégée. La vulnérabilité à 51% fait encore aujourd'hui l'objet de vifs débats concernant la gravité de ses conséquences potentielles.

Il est intéressant de noter que des événements récents pourraient rendre obsolètes les débats sur les attaques dites « à 51% ». Dans un article publié en août 2018, Vitalik Buterin, cofondateur d'Ethereum, propose un nouvel algorithme de consensus qui n'exigerait que 1% de nœuds honnêtes et écarterait le risque d'attaque à 51% (Buterin, 2018). En d'autres termes, un attaquant qui veut contrôler le réseau devrait contrôler 99% des nœuds de la chaîne de blocs, et pas seulement 51%. L'attaque à 51% pourrait bientôt être appelée attaque à 99%.

(a) Chaîne de blocs ou technologie de registres distribués

Parce qu'elle est simple et accrocheuse, l'expression « chaîne de blocs » est souvent utilisée pour désigner les registres distribués quelles que soient leurs caractéristiques particulières. Or la chaîne de blocs n'est qu'un type de technologie de registres distribués – une technologie qui regroupe les transactions dans des blocs qui sont ensuite enchaînés les uns aux autres. La chaîne de blocs est la technologie de registres distribués la plus connue et la plus éprouvée, mais de nombreux modèles de flux de transactions sont actuellement développés qui, comme la chaîne de blocs, utilisent diverses techniques cryptographiques, mais qui s'écartent du concept de « blocs », et même à la fois des concepts de « chaîne » et de « blocs ». Parmi ces nouveaux modèles, on peut citer IOTA¹¹, Ripple¹² et Hashgraph.¹³ Bien que ces nouveaux modèles ne soient pas des chaînes de blocs à proprement parler, l'expression « chaîne de blocs » est maintenant employée pour désigner en général la technologie des registres distribués et le phénomène qui l'accompagne. Pour faciliter la lecture, l'expression « chaîne de blocs » est utilisée ici, comme dans beaucoup d'autres publications, pour désigner plus généralement la « technologie des registres distribués ».

3. Types de chaînes de blocs

Derrière l'expression simple et accrocheuse de « chaîne de blocs », il y a en réalité de nombreux modèles différents qui varient par le degré de décentralisation et d'accès, l'identité des participants, le mécanisme de consensus, la rapidité, le niveau de confidentialité, la consommation d'énergie, les frais et la scalabilité (voir le tableau 1).

Tableau 1 Aperçu des principales caractéristiques des différents types de chaînes de blocs

Degré de centralisation	Publique			Consortium		Privée
Gestion	Pas de gestion centralisée			Organisations multiples		Entité unique
Accès	Sans permission	Avec permission	Avec permission	Avec permission	Sans permission	Avec permission
Participants	Lecture libre/validation libre des transactions	Lecture libre/validation des transactions avec permission	Lecture libre/validation OU libre/validation des transactions avec permission	Lecture avec permission OU libre/validation des transactions avec permission	Lecture libre/validation libre des transactions	Lecture/validation des transactions avec permission
	Anonymes / pseudonymes	Anonymes / pseudonymes	Identifiés	Identifiés	Généralement identifiés	Identifiés
Validation basée sur un protocole de consensus	Ouverte à tous les membres du réseau	Ouverte à tous les membres du réseau, sous certaines conditions	Par des membres préalablement approuvés (parmi les organisations participantes)	Par des membres préalablement approuvés	Dépend du protocole de consensus choisi pour la plate-forme	Par des membres préalablement approuvés (au sein de l'entité unique)
Vitesse de validation	Lente	Plus rapide	Rapide	Rapide	Rapide	Rapide
Niveau de confidentialité des utilisateurs	Aucun	Aucun	Adapté aux besoins des participants	Adapté aux besoins des participants	Adapté aux besoins des participants	Adapté aux besoins des participants
Puissance de calcul nécessaire (consommation d'énergie)	Importante (mais variable selon le mécanisme de consensus)	Moyenne	Plus faible	Plus faible	Plus faible	Plus faible
Frais de transaction	Oui	Oui	Facultatifs, selon les règles de la chaîne de blocs	Facultatifs, selon les règles de la chaîne de blocs	Facultatifs, selon les règles de la chaîne de blocs	Facultatifs, selon les règles de la chaîne de blocs
Scalabilité	Faible	Légèrement plus élevée	Plus élevée	Plus élevée	Plus élevée	Plus élevée
Exemple(s)	Preuve de travail (Bitcoin, Ethereum)	Preuve de participation (Nxt)	Chaînes de blocs basées sur Hyperledger Fabric	Chaînes de blocs basées sur permission basées sur Ethereum	FastTrackTrade	Chaînes de blocs privées basées sur Ethereum

Source : Auteure.

On établit souvent une distinction entre les chaînes de blocs publiques et les chaînes de blocs privées, dont un sous-type est appelé chaîne de blocs de consortium ou fédérée, et est parfois considéré comme une chaîne de blocs à part entière (Buterin, 2015). Une autre classification courante des applications de la chaîne de blocs fait une distinction entre les plates-formes sans permission et avec permission, c'est-à-dire que l'accès à la plate-forme est limité – ou non – à ceux qui ont une autorisation. Ces deux classifications sont parfois confondues, et il n'est pas rare que l'on pense que les chaînes de blocs publiques sont accessibles sans permission et que les chaînes de blocs privées ou de consortium nécessitent une permission. La réalité est cependant un peu plus complexe, car l'accès à certaines chaînes de blocs publiques peut nécessiter une permission.

Le monde des chaînes de blocs est nébuleux, complexe et en évolution rapide. Les définitions et les classifications ne sont pas gravées dans le marbre, mais évoluent sans cesse à mesure que la technologie mûrit et que de nouveaux modèles de flux de transactions et d'applications sont mis au point.

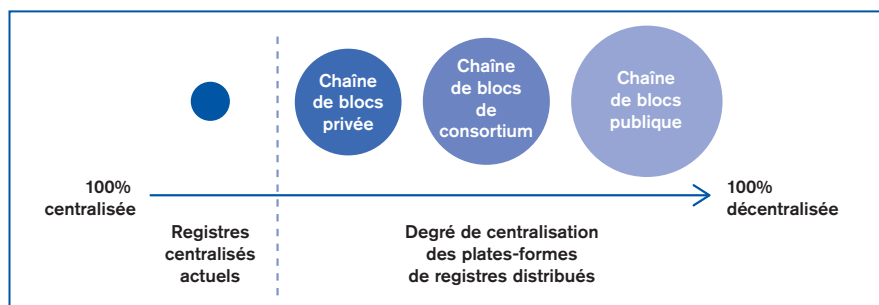
(a) Chaînes de blocs accessibles avec ou sans permission

La distinction entre les chaînes de blocs avec ou sans permission est liée principalement à la question de l'accès à la plate-forme. Une chaîne de blocs sans permission est ouverte à toute personne ayant un ordinateur : tout un chacun peut accéder à la plate-forme et valider des transactions.

En revanche, l'accès à une chaîne de blocs nécessitant une permission est restreint. L'accès peut être limité à différents niveaux en fonction des spécificités de la plate-forme (chaîne de blocs publique, gérée par un consortium ou privée), et selon qu'il s'agit de lire des données, de proposer une nouvelle transaction ou de valider des transactions (BitFury Group, 2015). Les chaînes de blocs sans permission, comme bitcoin, sont celles qui font la une des journaux, mais de nombreux cas d'utilisation dans le domaine du commerce international concernent des chaînes de blocs soumises à autorisation.

(b) Chaînes de blocs publiques ou chaînes de blocs privées de consortium

La distinction entre les chaînes de blocs publiques, gérées par un consortium et privées est liée à la question de la gouvernance de la plate-forme (qui la gère) et de l'authentification des utilisateurs (degré d'anonymat des participants). Ces différents types de plates-formes se distinguent par leur degré de décentralisation (voir la figure 2).

Figure 2 Le degré de décentralisation des registres distribués varie

Source : Auteure.

(i) Les chaînes de blocs publiques

Dans une plate-forme publique, aucune entité particulière ne gère la plate-forme, les transactions sont publiques et les utilisateurs peuvent garder l'anonymat. Aucun utilisateur n'a de privilèges spéciaux en matière de décision. Le système ne recourt plus à des tiers de confiance pour valider les transactions, mais se base sur les nœuds pour générer un consensus avant que les données (enregistrement d'une transaction, bloc, etc.) soient stockées dans le registre.

Toutefois, les plates-formes publiques ont besoin que les utilisateurs soient incités à parvenir à un consensus. Sur la chaîne de blocs Bitcoin, par exemple, le processus de vérification nécessite la résolution de problèmes mathématiques complexes. Le mineur*, c'est-à-dire le « validateur » qui résout le premier le problème mathématique, est récompensé par des bitcoins. Les frais imposés en contrepartie aux utilisateurs varient considérablement d'une plate-forme à l'autre. Ils sont, de loin, les plus élevés sur la plate-forme Bitcoin.¹⁴ Au début de novembre 2017, les frais moyens pour les transactions en bitcoins s'élevaient à plus de 11 \$EU par transaction, ce qui a amené certains membres de la communauté à affirmer que le système avait atteint ses limites (voir le tableau 2 de la section 4.2 a), ainsi que Redman (2017), Chaparro (2017) et Bershidsky (2017)).

La plupart des chaînes de blocs sont accessibles sans permission, c'est-à-dire qu'elles sont ouvertes à tous. Par conséquent :

- tout un chacun peut télécharger le logiciel nécessaire sur son ordinateur sans autorisation et peut commencer à exécuter un nœud public, valider des transactions et participer ainsi au protocole de consensus, qui détermine quels blocs sont ajoutés à la chaîne ;

- tout un chacun peut envoyer des transactions sur le réseau ; et
- tout un chacun peut lire et écrire des données pertinentes sur la chaîne de blocs.

Les chaînes de blocs publiques sans permission sont l'application la plus proche de ce pour quoi la technologie a été conçue initialement par Bitcoin. Les cryptomonnaies, et le bitcoin en particulier, sont l'illustration la plus typique des chaînes de blocs publiques sans permission.

Toutefois certaines chaînes de blocs publiques nécessitent une permission. Par exemple, dans le cas du protocole de preuve de participation* – que Ethereum, la deuxième grande chaîne de blocs publique, a l'intention d'introduire en 2018 –, seules les personnes remplissant certaines conditions préalables peuvent valider les transactions en fonction de leur « participation » dans la chaîne de blocs (en particulier le nombre d'unités qu'elles possèdent et depuis combien de temps).

En raison de leur nature très décentralisée, les chaînes de blocs publiques sont considérées comme particulièrement sûres et résistantes aux attaques malveillantes, sans point de défaillance unique*, mais elles sont confrontées à des problèmes de scalabilité (voir la section 4.2 a)).

(ii) Les chaînes de blocs privées

Dans les chaînes de blocs entièrement privées, les permissions nécessaires pour valider et écrire des données dans la chaîne de blocs sont contrôlées par une entité à laquelle les autres utilisateurs font entièrement confiance, et l'identité des participants est connue. Dans certaines situations, l'entité peut limiter la permission de lecture à certains utilisateurs. Ces permissions restreintes assurent plus de confidentialité aux utilisateurs, fonction qui n'est pas disponible dans les chaînes de blocs publiques. L'entité chargée du contrôle a le pouvoir de modifier les règles de la chaîne de blocs privée et peut refuser des transactions sur la base des règles établies.

Dans une chaîne de blocs privée, les transactions sont vérifiées par un nombre très restreint de nœuds (selon les règles de la chaîne), ce qui assure une plus grande efficacité et permet le traitement beaucoup plus rapide des transactions que dans les chaînes de blocs publiques, tout en nécessitant beaucoup moins de puissance de calcul. Des frais de transaction peuvent s'appliquer pour la validation des transactions selon les règles de la chaîne de blocs.

En outre, étant donné que les validateurs sont connus, il est plus facile de réparer les nœuds défectueux par une intervention humaine, et le risque d'une attaque à 51% ou à 99% lié à la collusion des mineurs n'existe pas ; mais la nature plus

centralisée de ces réseaux les rend moins résistants aux attaques extérieures et il y a un plus grand risque de manipulation humaine des données.

L'emploi de l'expression « chaîne de blocs » dans le contexte des registres privés est controversée et contestée, car les registres très centralisés ont peu en commun avec l'idée initiale de la chaîne de blocs.

(iii) Les chaînes de blocs de consortium

Une chaîne de blocs de consortium est un type de chaîne de blocs privée qui fonctionne sous la conduite d'un groupe plutôt que d'une entité unique, et dans laquelle l'identité des participants est connue. C'est une plate-forme « partiellement décentralisée » (Buterin, 2015).

Au lieu de permettre à toute personne disposant d'une connexion Internet de participer au processus de vérification des transactions ou de laisser une seule entité avoir le plein contrôle, quelques nœuds sélectionnés sont préalablement définis. Ces nœuds contrôlent le processus de consensus. Ils peuvent lire et/ou écrire les données et décider qui a accès au registre de la chaîne de blocs. Le droit de lire la chaîne de blocs peut être public ou limité aux participants (Buterin, 2015).

Par exemple, une chaîne de blocs de consortium peut être formée entre dix entreprises, chacune exploitant un dispositif connecté au réseau de la chaîne de blocs. Si l'entreprise 2 échange et partage ses factures uniquement avec les entreprises 3, 4 et 5, il peut être décidé que la permission de lire les données partagées ne sera donnée qu'à ces entreprises.

Bien souvent, ces plates-formes sont utilisées pour tirer parti des caractéristiques spécifiques de la technologie des registres distribués, pour renforcer la coopération et pour améliorer les processus entre des institutions, comme les banques, les entreprises et les organismes publics. Hyperledger Fabric, par exemple, est une application de la chaîne de blocs développée par IBM et donnée au projet Hyperledger de la Fondation Linux, qui a été conçu pour développer des chaînes de blocs avec permission répondant aux besoins des entreprises participantes.¹⁵

Les chaînes de blocs privées et de consortium ne sont généralement accessibles qu'avec une permission, ce qui permet aux institutions participantes de maintenir un certain degré de contrôle et de confidentialité. Les chaînes de blocs de consortium avec permission sont largement utilisées dans le domaine du commerce international, non sans raison car de nombreuses institutions ne souhaitent pas mettre des renseignements commerciaux privés sur une chaîne de blocs publique accessible à tous sans permission. Certaines chaînes de blocs privées de consortium

peuvent cependant être ouvertes à toute personne intéressée. Une plate-forme comme FastTrackTrade¹⁶, qui utilise la technologie de la chaîne de blocs pour construire un réseau commercial numérique pour les micro, petites et moyennes entreprises (MPME) de Singapour, est ouverte à toutes les entreprises intéressées – mais on pourrait objecter que seules les entreprises peuvent y accéder. En outre, les chaînes de blocs privées ou de consortium avec permission peuvent avoir une interface publique, c'est-à-dire que tout le monde peut lire les données.

Ces classifications rendent compte des caractéristiques essentielles des principaux types de chaînes de blocs, mais il existe de nombreuses variantes. La manière dont les chaînes de blocs sont conçues dépend des objectifs recherchés et du degré de décentralisation et de confidentialité souhaité.

4. Les contrats intelligents : une invention intelligente sans composante intelligente

Les contrats intelligents sont l'une des caractéristiques les plus intéressantes de la technologie de la chaîne de blocs, en particulier dans le contexte du commerce international. Il ne s'agit pas d'un type de chaîne de blocs en soi, mais c'est plutôt une fonctionnalité de la technologie de la chaîne de blocs.

En fait, l'expression « contrat intelligent » est mal choisie : les contrats intelligents ne sont ni « intelligents » (il n'y a aucune composante cognitive ni aucun élément d'intelligence artificielle ; c'est seulement l'exécution automatique d'une tâche prédéfinie lorsque certaines conditions sont remplies) ni des contrats au sens juridique du terme (Deloitte, 2018).

Les contrats intelligents sont des programmes informatiques qui s'exécutent automatiquement (auto-exécution) sans l'intervention d'un tiers lorsque des conditions spécifiques sont remplies (selon la logique « si... alors... », par exemple, si les marchandises sont déchargées au port de X, alors les fonds seront transférés). Ils énoncent les obligations de chaque partie au « contrat », ainsi que les avantages ou les pénalités possibles pour telle ou telle partie dans différentes circonstances.

À la différence des contrats juridiques traditionnels, les contrats intelligents gèrent l'information comme une entrée, la traitent selon les règles établies dans le contrat, puis exécutent une action convenue. Cette information est inscrite dans le contrat intelligent par des « oracles »*, c'est-à-dire des flux de données, fournies par des prestataires de services tiers, sur les conditions prédéfinies prévues dans le contrat intelligent. Il peut s'agir de données externes telles que la température, l'exécution du paiement et les variations de prix. Un contrat d'assurance intelligent pourrait, par

exemple, avoir comme oracle un capteur placé dans un conteneur réfrigéré. Si la température dépasse un certain niveau, les paiements d'assurance seraient automatiquement déclenchés et une demande d'inspection serait envoyée. Étant donné que les chaînes de blocs ne peuvent pas accéder aux données en dehors de leur réseau, les oracles sont le seul moyen pour les contrats intelligents d'«interagir» avec les données extérieures à l'environnement de la chaîne de blocs. En d'autres termes, les contrats intelligents fonctionnent généralement en conjonction avec d'autres technologies, en particulier l'Internet des objets, c'est-à-dire des réseaux de capteurs et de dispositifs intelligents connectés à Internet et capables d'envoyer et de recevoir des données. Les contrats intelligents utilisent généralement les données générées par l'Internet des objets pour déclencher des actions.

Le concept de contrats intelligents a été présenté et développé par le cryptographe Nick Szabo dans diverses publications parues entre 1994 et 1997 et a été introduit pour la première fois dans le contexte de la technologie de la chaîne de blocs par Ethereum en 2015.¹⁷ Aujourd'hui, de nombreuses chaînes de blocs offrent des capacités de contrats intelligents. Des contrats intelligents peuvent exister en dehors de la chaîne de blocs, mais ils conservent alors les mêmes problèmes potentiels que les bases de données centralisées, c'est-à-dire un point de défaillance unique et la possibilité de modifier facilement les données.

La nature automatique des contrats intelligents en fait un outil particulièrement intéressant pour le commerce international, car il permet d'automatiser les transactions. Toutefois, l'utilisation de ces contrats soulève certaines questions juridiques qu'il est important de garder à l'esprit, en particulier des questions d'exécution et de responsabilité qu'il peut être nécessaire de régler si le contrat a été mal codé (voir la section 4.2. c)). De plus, les contrats intelligents sont des programmes informatiques et, comme tout code de programmation, ils peuvent contenir des erreurs involontaires (Delmolino *et al.*, 2015). L'attaque de 2016 contre une DAO mentionnée plus haut était due à une vulnérabilité dans le code de programme du contrat intelligent utilisé dans ce cas. Les contrats intelligents sont, avec l'interface utilisateur (c'est-à-dire le téléphone mobile, la tablette ou l'ordinateur utilisé pour accéder à Internet), la couche où la plupart des failles de sécurité se produisent dans l'écosystème des chaînes de blocs.

5. Des applications multiples... mais pas une solution pour tout

Alors que pour beaucoup, la chaîne de blocs «est au Bitcoin ce qu'Internet est au courriel électronique», comme l'a dit Sally Davies, journaliste spécialisée à FT Technology, cette technologie n'est pas seulement l'infrastructure qui sous-tend le

bitcoin. Ces dernières années ont montré qu'elle peut être appliquée à une grande variété d'industries et de secteurs, ayant chacun ses propres spécificités. Elle peut être déployée avec des fonctionnalités personnalisées. Des propriétés comme les exigences de sécurité ou les protocoles de consensus peuvent être adaptées aux besoins particuliers et aux exigences opérationnelles d'un projet particulier. Les services de développement de chaînes de blocs personnalisées se sont multipliés ces dernières années, offrant aux clients un large éventail de possibilités, y compris des interfaces préconçues ou des systèmes conçus totalement sur mesure, et les plates-formes libres (telles qu'Ethereum et Hyperledger Fabric) offrent aux développeurs la possibilité de construire des chaînes de blocs sur mesure en choisissant dans un menu de fonctionnalités et de protocoles.

Toutefois, malgré ses caractéristiques intéressantes, la chaîne de blocs ne peut pas tout régler, comme l'engouement actuel qu'elle suscite nous porte à le croire. Les entreprises et les institutions intéressées par cette technologie doivent réfléchir aux coûts et aux avantages de son utilisation et s'assurer qu'elle répond bien à leurs besoins. La construction d'une plate-forme de chaînes de blocs doit être mûrement pensée et bien coordonnée par les participants potentiels afin d'analyser les possibilités et les limites de la chaîne de blocs par rapport à d'autres options moins ambitieuses et de convenir des paramètres clés (par exemple la nature de la chaîne de blocs, les règles de validation, etc.), sans parler des connaissances technologiques dont les utilisateurs du système ont besoin. Une pléthore de modèles d'arbre décisionnel a été publiée sur le Web pour permettre aux entreprises et aux institutions de décider en connaissance de cause si une chaîne de blocs est une solution adaptée à leurs besoins et, le cas échéant, quel type de chaîne de blocs est le plus approprié pour leur situation.¹⁸

Note de fin

1. Le concept de chaîne de blocs sécurisée par cryptographie a été décrit pour la première fois en 1991 par Haber et Stornetta (1991), mais ce n'est qu'en 2008-2009 que la technologie a été effectivement appliquée.
2. Une cryptomonnaie est une monnaie numérique qui utilise la cryptographie à des fins de sécurité. Voir Nakamoto (2008).
3. Une monnaie fiduciaire est une monnaie qu'un gouvernement a déclaré avoir cours légal, mais qui n'est pas adossée à un produit physique, comme l'or ou l'argent.
4. Une organisation autonome décentralisée (DAO) est une organisation qui s'exécute de façon autonome selon les règles définies dans les contrats intelligents. Pour plus d'informations, voir: <https://blockchainhub.net/dao-decentralized-autonomous-organization/>.
5. Un compte bloqué est un compte financier spécial sur lequel des fonds sont déposés temporairement avant d'être versés (ou restitués) à la fin d'une transaction.
6. En ingénierie des logiciels et des systèmes, un cas d'utilisation est un terme qui décrit comment un système est utilisé pour atteindre un objectif particulier (définition de Techopedia).
7. Voir <https://www.iota.org/>.
8. Corda est un registre partagé et non un registre distribué. Contrairement aux réseaux de chaînes de blocs, qui reproduisent les données pour chaque membre du réseau, sur la plate-forme Corda, seules les parties ayant un besoin légitime de savoir peuvent accéder aux données dans le cadre d'un accord (voir «<http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services>»).
9. Voir <https://www.hyperledger.org/about>.
10. L'expression «chaîne de blocs» peut désigner la technologie de la chaîne de blocs elle-même, ou une application utilisant cette technologie, c'est-à-dire une plate-forme ou un réseau d'utilisateurs spécifiques (appelés nœuds), pour fournir un service particulier.
11. Lancé en 2016 en tant que cryptomonnaie conçue pour l'Internet des objets, IOTA est un registre public sans chaînes ni blocs ni frais. Il utilise une nouvelle technologie appelée Tangle (enchevêtrement): au lieu d'être regroupées en blocs et enchaînées les unes aux autres, les transactions IOTA sont connectées dans un vaste réseau enchevêtré (voir <https://iota.readme.io/docs/what-is-iota>).
12. Lancé en 2012, le protocole Ripple est destiné à permettre le transfert de fonds quasi instantané et direct entre deux parties dans n'importe quel type de monnaie. Bien qu'il soit consensuel, Ripple n'est techniquement pas une chaîne de blocs. Il condense les données en une valeur unique plutôt qu'en un bloc.
13. Hashgraph est une nouvelle alternative consensuelle à la chaîne de blocs qui ne regroupe pas les transactions en blocs. Il utilise un protocole consensuel qui, selon ses développeurs, est plus rapide, plus équitable et plus sûr que la chaîne de blocs et qui a conduit de nombreux observateurs à se demander si Hashgraph n'avait pas rendu la chaîne de blocs obsolète. Toutefois, ce n'est pas encore un logiciel libre, et il faut encore procéder à une analyse et à une évaluation comparative adéquates avant que de telles affirmations puissent être confirmées.

14. En fait, dans le cas de Bitcoin, le système tel qu'il était conçu à l'origine prévoyait que les frais de transaction seraient facultatifs, du moins tant que les mineurs seraient récompensés par des bitcoins (le bitcoin étant volontairement conçu comme déflationniste, le nombre d'unités créées dans le système est limité et la monnaie est appelée, à terme, à manquer). Cependant, il ressort de rapports récents que non seulement les frais de transaction sont devenus pratiquement la seule façon pour les utilisateurs de faire entrer leurs transactions dans les blocs, mais que le montant des frais pour le bitcoin a grimpé en flèche. Les scénarios sont assez différents et moins dramatiques pour d'autres plates-formes de cryptomonnaies.

15. Voir <https://www.hyperledger.org/projects/fabric>.

16. Voir <https://www.fasttracktrade.co>.

17. Szabo a défini les contrats intelligents comme suit: «Un contrat intelligent est un protocole de transaction informatisé qui exécute les clauses d'un contrat. Les objectifs généraux de la conception de contrats intelligents sont de satisfaire aux conditions contractuelles courantes (comme le paiement des termes, les gages, la confidentialité et même l'exécution), de limiter les exceptions malveillantes et accidentelles et de réduire le besoin d'intermédiaires de confiance. Les objectifs économiques connexes comprennent la réduction des pertes dues à la fraude, les coûts d'arbitrage et d'exécution et les autres coûts de transaction» (cité dans Tapscott et Tapscott, 2018).

18. Voir, par exemple, le modèle d'arbre d'IBM présenté à l'adresse <https://www.altoros.com/blog/howhyperledger-fabric-delivers-security-to-enterprise-blockchain/>, ou le modèle du livre blanc du Forum économique mondial disponible à l'adresse: http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf.

3

La chaîne de blocs peut-elle révolutionner le commerce international ?

Les gros titres annonçant que la chaîne de blocs peut révolutionner différents domaines du commerce international, du financement du commerce aux procédures douanières, en passant par la propriété intellectuelle, sont légion. Le caractère transparent, décentralisé et immuable de la chaîne de blocs a éveillé l'intérêt des acteurs privés – et des gouvernements – qui veulent explorer le potentiel de cette technologie afin d'améliorer l'efficacité des processus commerciaux, et une multitude de preuves de concept et de projets pilotes utilisant la chaîne de blocs ont été menés dans quasiment tous les domaines du commerce international.

La chaîne de blocs a-t-elle réellement la capacité de révolutionner le commerce international ? Le présent chapitre étudie la pertinence de la chaîne de blocs pour les transactions commerciales transfrontières. Il examine de quelle manière la technologie de la chaîne de blocs peut influencer sur les différentes étapes du commerce international des marchandises, du financement du commerce aux procédures douanières, en passant par la certification, le transport et la logistique, et aider à avancer vers une plus grande numérisation du commerce. Le présent chapitre analyse également le potentiel de la chaîne de blocs dans d'autres domaines couverts par l'OMC, en mettant en particulier l'accent sur certains secteurs clés des services, la propriété intellectuelle et les marchés publics.

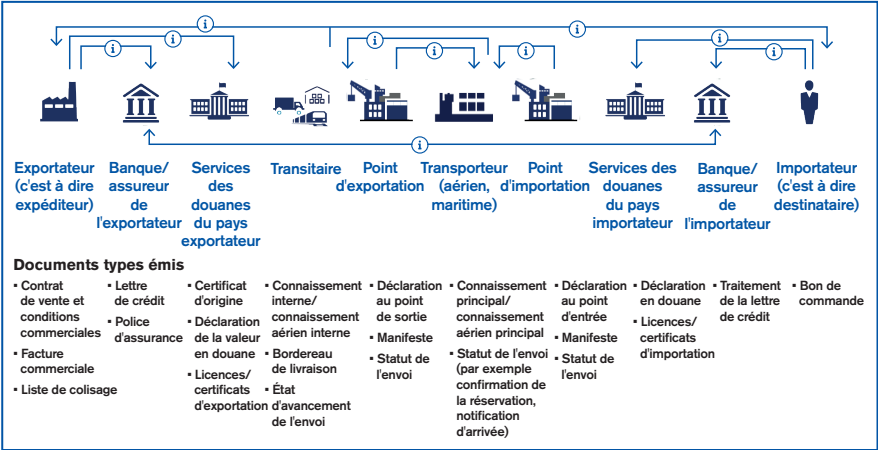
1. Vers un commerce sans papier ?

Les transactions commerciales internationales font intervenir de multiples d'acteurs et reposent encore très largement sur le papier. En 2014, la compagnie de transport Maersk a suivi un conteneur réfrigéré rempli de roses et d'avocats depuis le Kenya jusqu'aux Pays-Bas dans le but de documenter le dédale de processus physiques et de formalités administratives que chaque envoi doit suivre. Les chiffres parlent d'eux-mêmes : environ 30 organismes et plus de 100 personnes sont intervenus tout au long du voyage, le nombre d'interactions excédant 200. Il a fallu environ 34 jours pour que l'envoi parvienne aux détaillants depuis l'exploitation agricole, dont 10 jours d'attente avant que certains documents ne soient traités. Il s'est avéré qu'il manquait l'un des documents clés ; il a par la suite été retrouvé au milieu d'une pile de papiers (Park, 2018).

Une multitude de documents doivent être présentés au cours d'une transaction commerciale internationale (voir la figure 3), qui peuvent être classées en quatre grandes catégories (voir la figure 4) :

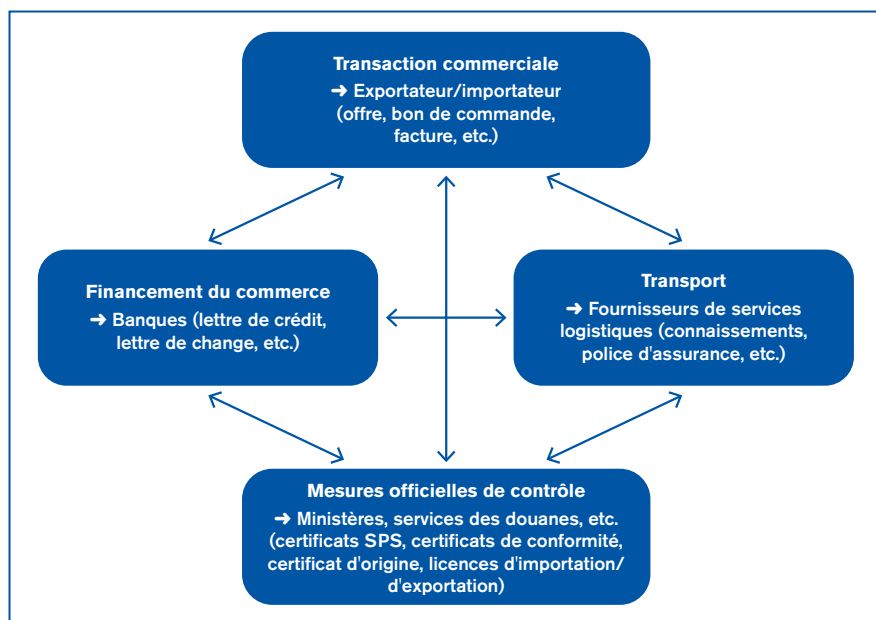
- documents liés à la transaction commerciale elle-même, y compris contrat de vente, factures commerciales et, si nécessaire, liste de colisage présentée par l'exportateur avant l'exportation;
- documents liés au financement du commerce, tels que lettres de crédit;
- documents de transport, y compris connaissements, etc.; et
- documents pour les procédures à la frontière, y compris :
 - certificats d'origine – délivrés par les chambres de commerce, bien que d'autres organismes tels que des ministères ou des autorités douanières puissent également avoir cette prérogative dans certains pays;
 - certificats sanitaires et phytosanitaires, dans le cas des produits alimentaires, végétaux et agricoles – généralement délivrés par les ministères de la santé ou de l'agriculture;
 - certificats de conformité qui certifient qu'un produit ou un service satisfait aux prescriptions d'une norme donnée dans le pays d'importation;
 - licences d'exportation ou d'importation, si les autorités du pays de l'exportateur ou de l'importateur en font la demande;
 - déclarations en douane;
 - documents d'inspection en douane.

Figure 3 Documents types émis dans le cadre du commerce international



Source : Accenture.

Figure 4 Quatre processus intervenant dans les transactions commerciales transfrontières



Source : Auteure.

Non seulement ces divers processus, qui nécessitent beaucoup de papier, accroissent les coûts de coordination et les coûts administratifs, mais ils exposent aussi à des erreurs, des pertes et de la fraude. Bien que des progrès notables aient déjà été accomplis, la numérisation complète des transactions commerciales transfrontières de marchandises n'est pas encore en vue. La complexité et les coûts associés au commerce international des marchandises ont conduit un nombre croissant d'entreprises et de gouvernements à examiner de quelle manière la chaîne de blocs pourrait être utilisée pour réduire les formalités administratives et améliorer les processus liés à l'exportation des marchandises, du financement du commerce aux procédures à la frontière, en passant par le transport, dans l'espoir de se rapprocher d'un commerce véritablement sans papier.

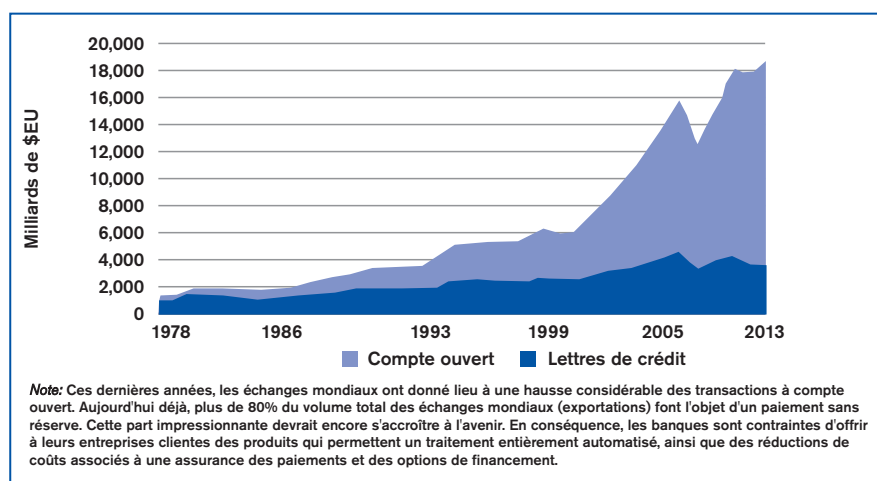
(a) La chaîne de blocs peut-elle faciliter le financement du commerce ?

La disponibilité du financement du commerce est essentielle pour les activités commerciales. Seule une petite partie des transactions commerciales internationales donnent lieu à un paiement d'avance en espèces car, généralement, les acheteurs

souhaitent payer seulement après que les marchandises ont été correctement livrées. Jusqu'à 80% du commerce est financé par une forme ou une autre de financement (OMC, 2016b), qui, d'une manière générale, inclut des mécanismes traditionnels, tels que les lettres de crédit, et le financement des chaînes d'approvisionnement – expression générique qui renvoie à un éventail d'instruments de financement utilisés pour financer des parties des chaînes d'approvisionnement. Même si les lettres de crédit ont traditionnellement été une forme de financement du commerce largement utilisée, il existe une tendance croissante à commercer à compte ouvert en utilisant le financement des chaînes d'approvisionnement (voir la figure 5).

Les mécanismes existants de financement traditionnel du commerce sont souvent associés à des coûts élevés et des procédures lourdes, en raison de processus nécessitant beaucoup de papier et de la difficulté de coordonner les multiples acteurs intervenant dans une transaction commerciale; le fait de commercer à compte ouvert¹ en utilisant des outils de financement des chaînes d'approvisionnement peut être un pari risqué pour les exportateurs, sans oublier les difficultés liées à la confiance, à la détection et à la prévention de la fraude, ainsi qu'à l'authentification des parties. Ces failles ont conduit les banques, les startups de technologie financière et les sociétés informatiques à étudier le potentiel de la chaîne de blocs pour la facilitation du financement du commerce. Cette technologie est considérée par beaucoup comme un outil intéressant pour améliorer la sécurité

Figure 5 Utilisation de lettres de crédit ou compte ouvert (volume des échanges mondiaux de 1978 à 2013)

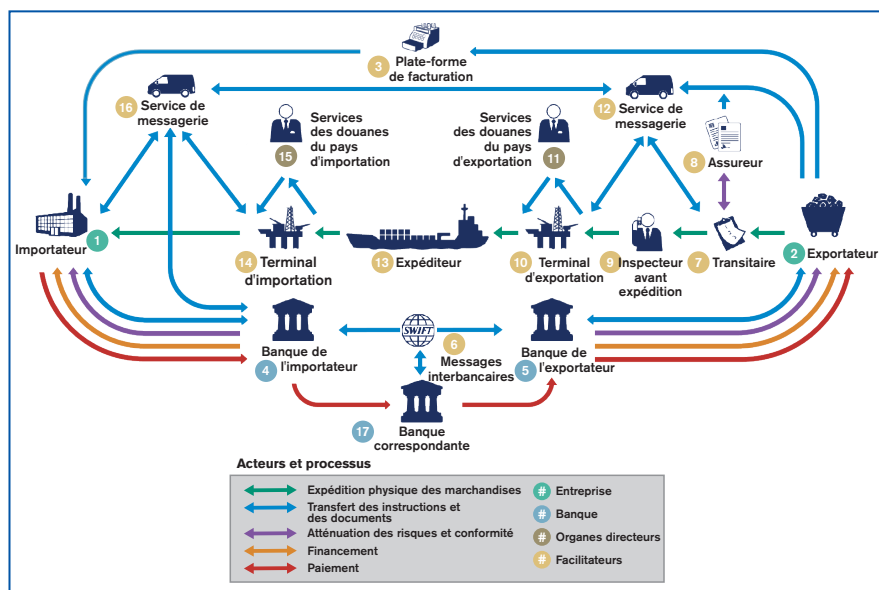


Source: Unicredit Group, cité dans CEFACT-ONU (à paraître).

des transactions de financement traditionnel du commerce, pour rationaliser et numériser les processus, en particulier les lettres de crédit, et pour faciliter les processus de connaissance du client et rendre plus aisé le financement des chaînes d'approvisionnement.

Le financement traditionnel du commerce – en particulier les transactions par lettres de crédit² – demande beaucoup de main-d'œuvre et de papier et fait intervenir de multiples acteurs. L'une des plus grandes banques fournissant un financement du commerce emploie plusieurs milliers de personnes pour vérifier chaque année des millions de documents commerciaux liés aux demandes de lettres de crédit, et des travaux de recherche récents menés par le Boston Consulting Group indiquent que plus de 20 acteurs sont généralement parties à une seule transaction de financement du commerce tout au long du processus, les données étant recueillies dans 10 à 20 documents, ce qui occasionne environ 5 000 interactions entre les champs de données (voir les figures 6 et 7). Seulement 1% de ces interactions créent de la valeur, 85% à 90% des transactions consistant en actions du type « ignorer/transmettre à la partie suivante » (Boston Consulting Group, 2017).

Figure 6 Le processus traditionnel de financement du commerce est très fragmenté entre de multiples entités et processus



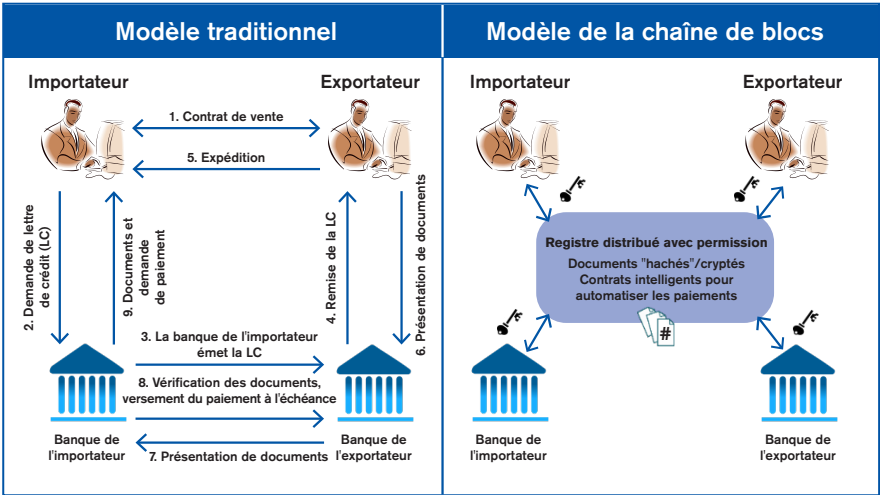
Source: Boston Consulting Group (2017).

Le système est coûteux et a conduit des banques et des entreprises telles que essDocs et Bolero à réfléchir à la manière dont les processus de financement du commerce pourraient être numérisés. Jusqu'à présent, les efforts se sont concentrés sur la numérisation des paiements et des renseignements, essentiellement par le biais de documents pdf numérisés. Toutefois, ils n'ont guère contribué à la numérisation des transactions elles-mêmes et à l'atténuation des risques liés au commerce (Castell, 2018). Le caractère transparent et sûr de la chaîne de blocs a soulevé des espoirs et conduit un nombre croissant de banques à réfléchir à la manière dont les chaînes de blocs pourraient contribuer à automatiser le processus, à améliorer l'efficacité des transactions et à renforcer la sécurité.

Plusieurs preuves de concept ont été menées ces quelques dernières années en vue de rationaliser et d'automatiser les processus liés aux lettres de crédit, et les applications de la chaîne de blocs dans ce domaine s'orientent désormais vers une application commerciale. En septembre 2016, Barclays et la startup de technologie financière Wave ont indiqué avoir mené à bien le premier accord en direct de financement du commerce basé sur la chaîne de blocs (Barclays, 2016). La transaction, effectuée par l'intermédiaire d'un registre avec permission, a garanti l'exportation de fromage et de beurre de la coopérative laitière irlandaise Ornua (anciennement Office irlandais des produits laitiers), pour un montant de presque 100 000 dollars, à destination des Seychelles. Selon Barclays, le processus de transaction par lettre de crédit qui, entre la délivrance et l'approbation, demande habituellement entre sept et dix jours, pourrait être réduit à moins de quatre heures. La lettre de crédit elle-même a été émise par l'intermédiaire du système de la Society for Worldwide Interbank Financial Telecommunication (SWIFT) et les fonds ont été débloqués de manière traditionnelle.

En août 2016, la Bank of America, HSBC et la Direction du développement de l'information et de la communication de Singapour (IDA) ont annoncé qu'elles avaient mis au point une application de chaîne de blocs fondée sur Hyperledger Fabric pour améliorer le processus de transaction par lettre de crédit. L'application reproduit une transaction par lettre de crédit traditionnelle en partageant les renseignements entre les exportateurs, les importateurs et leurs banques respectives dans un registre distribué avec permission (voir la figure 8). Une série de contrats numériques intelligents* leur permet d'exécuter l'accord automatiquement (HSBC, 2016). En outre, en mai 2018, HSBC a réalisé ce qu'elle estime être la « première transaction du monde en matière de financement du commerce viable sur le plan commercial » utilisant la chaîne de blocs, ouvrant peut-être la voie à une utilisation commerciale de la technologie pour les opérations de financement du commerce (Weinland, 2018). La transaction par lettre de crédit du groupe américain Cargill portant sur un envoi de fèves de soja depuis l'Argentine vers la Malaisie a été réalisée sur la plate-forme basée sur la chaîne de blocs Voltron

Figure 8 Exemple de processus de lettre de crédit^a



^a Les fonctionnalités spécifiques des plates-formes de chaînes de blocs (par exemple types de paiements) dépendent des caractéristiques choisies par les participants.

Source: Auteure.

dédiée aux lettres de crédit construite par un groupe de onze banques à partir de la plate-forme Corda développée par le consortium R3.

Au-delà des efforts visant à exploiter la capacité de la technologie d'améliorer les processus de financement traditionnel du commerce existants tels que les lettres de crédit, le caractère disruptif de la technologie conduit certaines entreprises à mettre au point de nouveaux produits et modèles de financement des chaînes d'approvisionnement.

Si les lettres de crédit restent importantes, un nombre croissant de transactions commerciales sont effectuées à compte ouvert en utilisant le financement des chaînes d'approvisionnement.³ Au sein de l'Union européenne, par exemple, les lettres de crédit sont en fait peu utilisées pour les échanges intrarégionaux. Ce n'est pas sans raison : le processus très lourd qu'elles impliquent demande généralement plus de temps que le délai nécessaire aux marchandises pour parvenir à destination. Les transactions à compte ouvert, en revanche, sont l'option la plus risquée pour l'exportateur : dans une transaction à compte ouvert, les marchandises sont expédiées et livrées avant que le paiement ne soit exigible.⁴

En décembre 2016, sept banques ont fait le pari de rendre le financement à compte ouvert moins risqué en utilisant la technologie de la chaîne de blocs, avec le

lancement du consortium Digital Trade Chain, depuis lors rebaptisé We.trade (Groenfeldt, 2017). We.trade est une «plate-forme centrée sur la banque», basée sur la chaîne de blocs, construite à partir de Hyperledger Fabric, qui regroupe neuf banques et recouvre onze pays de l'UE (données de juillet 2018).⁵ Les négociants s'enregistrent sur la plate-forme par l'intermédiaire de leurs banques. Les importateurs et les exportateurs peuvent alors enregistrer leurs transactions sur la plate-forme après être convenus des modalités du contrat (marchandises considérées, prix, délai de paiement, conditions de règlement). Un contrat intelligent assure une garantie de paiement et un règlement automatique lorsque les conditions déterminées entre les parties sont satisfaites. Les paiements peuvent s'effectuer à compte ouvert ou via un engagement de paiement d'une banque (Bank Payment Undertaking ou BPU), c'est-à-dire une garantie de paiement bancaire. La plate-forme a réalisé ses premières opérations en direct en juillet 2018, avec la participation de 20 entreprises et 5 grandes banques (Suberg, 2018).

L'initiative We.trade n'est que l'un des nombreux projets qui prolifèrent de par le monde. Par exemple, IBM s'est récemment associé avec la société indienne Mahindra⁶ et le conglomérat chinois Sichuan Hejia⁷ pour élaborer de nouvelles solutions basées sur la chaîne de blocs avec permission pour le financement des chaînes d'approvisionnement, tandis que la société Dianrong, chef de file sur le marché du prêt en ligne, basée en Chine, et la société FnConn (filiale de Foxconn) ont uni leurs efforts pour lancer ChainedFinance en mars 2017.⁸ D'autres exemples incluent le partenariat entre Mizuho Financial Group et Hitachi, le projet Eximchain soutenu par le MIT (Huertas, Liu et Robinson, 2018), et la plate-forme Marco Polo lancée en septembre 2018.

Toutes ces plates-formes exploitent la technologie de la chaîne de blocs et des contrats intelligents pour rationaliser les flux financiers entre les acheteurs, les vendeurs et les financiers, et améliorer la sécurité, la rapidité, la transparence et la fiabilité du financement des chaînes d'approvisionnement. Des études récentes montrent que la chaîne de blocs peut effectivement procurer des avantages substantiels à toutes les parties impliquées dans la transaction de financement de la chaîne d'approvisionnement, en accélérant les processus et en réduisant les coûts globaux des programmes de financement. (Hofmann, Strewe et Bosia, 2017). Ces initiatives ouvrent des possibilités particulièrement intéressantes pour les micro, petites et moyennes entreprises (MPME), qui ont souvent des difficultés à obtenir un financement du commerce en raison de l'absence de nantissement suffisant ou d'antécédents en matière de crédit médiocres ou inexistants. En donnant aux financiers une plus grande visibilité sur la trésorerie de la chaîne d'approvisionnement et les antécédents des entreprises en matière de crédit, la chaîne de blocs peut faciliter les processus de connaissance du client et rendre plus aisé l'accès des MPME à un financement abordable.⁹

L'utilisation de la technologie de la chaîne de blocs pour les opérations de financement du commerce a également suscité l'intérêt des autorités monétaires. En mars 2017, l'autorité monétaire de Hong Kong a dévoilé une plate-forme de financement du commerce utilisant la technologie de la chaîne de blocs (Perez, 2017), alors que l'autorité monétaire de Singapour collabore avec le Centre IBM pour l'innovation basée sur la chaîne de blocs afin d'élaborer des applications et des solutions utilisant la chaîne de blocs pour améliorer l'efficacité des processus et transactions de financement du commerce (IBM, 2016). En novembre 2017, ces derniers ont annoncé un projet conjoint visant à développer un réseau mondial de connectivité commerciale, une infrastructure transfrontières basée sur la chaîne de blocs permettant de numériser le commerce et le financement du commerce entre Hong Kong, Chine et Singapour. À terme, l'objectif est d'étendre le réseau à la région et au monde entier. La plate-forme devrait entrer en service au début de l'année 2019. La banque centrale de Chine est également à l'origine d'une plate-forme de financement du commerce visant à fournir un financement des chaînes d'approvisionnement dans la région de la baie de Guangdong-Hong Kong, Chine-Macao, Chine dans le but d'aider les petites et moyennes entreprises à accéder au financement du commerce (Huillet, 2018a).

L'engouement est réel, mais certains restent sceptiques au vu de l'effervescence qui a entouré les obligations bancaires de paiement (OBP) il y a quelques années. Lancées par SWIFT en 2013, les OBP sont des garanties de paiement conditionnelles fournies par une banque à une autre. À la différence des lettres de crédit, qui nécessitent beaucoup de papier, les OBP utilisent l'appariement électronique des données pour faciliter les paiements entre la banque d'un importateur et la banque d'un exportateur. Lorsqu'elles ont été lancées, les OBP ont été saluées comme un moyen nouveau et révolutionnaire d'optimiser les flux de financement du commerce. Bien que plus rapides et moins coûteuses que les lettres de crédit, les OBP n'ont pourtant été utilisés qu'à une échelle limitée. Diverses raisons ont été invoquées face à ce manque d'intérêt : chaque partie à la transaction devait pouvoir utiliser les OBP, l'investissement dans la technologie pouvait être coûteux et le passage aux OBP demandait un remaniement des processus traditionnels bien établis et un changement de culture.

La chaîne de blocs a-t-elle de meilleures chances de réussir que les OBP ? Les avis divergent, en particulier lorsqu'il s'agit des lettres de crédit. Certains observateurs notent, par exemple, que la source la plus importante de fraude en matière de lettres de crédit est la délivrance de faux documents et non la falsification de documents, une question que la chaîne de blocs ne peut pas résoudre, car la technologie ne peut empêcher l'introduction de faux renseignements dans le registre (Takahashi, 2018). La vérification des documents demeurera donc nécessaire. En outre, le paiement au titre d'une lettre de crédit est déjà souvent effectué par virement électronique.

D'autres cependant notent que les registres distribués offrent de nouveaux avantages potentiels, y compris une cybersécurité accrue, une plus grande transparence, des transactions en temps réel, des paiements automatiques au moyen de contrats intelligents, une vérification facile des transactions en raison du caractère transparent et immuable de la technologie, et l'inclusion facile de participants additionnels. Les partisans de la chaîne de blocs estiment que la technologie offre la meilleure solution possible pour numériser le financement du commerce, ce qui conduit même certains à affirmer que l'OBP se transformera en « obligation de paiement par la chaîne de blocs », selon les termes de Wassilios Lytras, cofondateur de Gatechain, une startup suisse qui développe des solutions basées sur la chaîne de blocs pour le financement du commerce.

Toutefois, la numérisation du financement du commerce par le biais de la chaîne de blocs, si elle se produit, n'interviendra pas du jour au lendemain. Premièrement, la technologie est encore à l'essai et des investissements importants sont encore nécessaires pour la rendre opérationnelle à plus grande échelle. Une évolution positive est que les différentes parties prenantes intervenant dans les transactions de financement du commerce unissent leurs forces. Les banques, les sociétés de technologie financière et d'autres acteurs forment des partenariats pour étudier conjointement le potentiel de la technologie et développer les applications les mieux adaptées aux besoins de leurs clients. Par exemple, comme indiqué au chapitre 2, la société R3 (R3CEV LL.) est une entreprise de technologie à la tête d'un consortium de plus de 200 établissements financiers et organismes de réglementation qui mène des activités de recherche-développement sur la chaîne de blocs dans le système financier, via sa propre plate-forme, Corda.¹⁰ En août 2017, un groupe de banques du consortium R3 a annoncé l'essai d'une plate-forme dédiée aux transactions par lettre de crédit (Persio, 2016). La plate-forme, appelée Voltron, est entrée dans sa deuxième phase pilote en septembre 2018 et devrait être disponible en 2019. Toutefois, la haute direction de R3 reconnaît que l'adoption généralisée ne sera pas possible avant cinq ou six ans (PalFREeman, 2017).

En septembre 2018, un consortium de dix banques du réseau R3 a lancé une autre plate-forme, Marco Polo, visant à prendre en charge le financement ouvert du commerce (Wass, 2018c).

Deuxièmement, il ne suffit pas que la technologie soit en place. Des cadres juridiques qui clarifient, par exemple, le statut juridique des documents électroniques, les règles et procédures de règlement des différends applicables lorsqu'un contrat intelligent est utilisé, et la responsabilité de chacun à chaque stade du processus, devront être élaborés. De la même manière que les lettres de crédit sont régies par un ensemble spécifique de règles convenues par la Chambre de commerce internationale (Règles et usances uniformes relatives aux crédits documentaires

– UCP 600) les contrats intelligents rendus possibles par la chaîne de blocs utilisés pour les transactions par lettre de crédit demanderont aussi un ensemble de règles convenues au niveau international, car les banques ne voudront peut-être pas s'engager avant que ces questions juridiques soient réglées. Le système actuel des lettres de crédit peut être extrêmement coûteux, mais il est efficace en termes de protection juridique. Des travaux sont en cours dans des instances telles que la Chambre de commerce internationale (ICC) et l'Organisation internationale de normalisation (ISO), mais l'élaboration de normes peut demander du temps (voir la section 4.2 c)).

Toutefois, la question de la responsabilité – à savoir qui est responsable à chaque stade du processus – ne s'applique pas dans les mêmes termes dans le cas de solutions visant la chaîne d'approvisionnement telles que celle élaborée par We.trade. En effet, une caractéristique intéressante de cette nouvelle approche est que les questions de responsabilité sont établies dans un contrat hors ligne entre l'acheteur et le vendeur. Les contrats intelligents ne sont utilisés que pour automatiser les processus et le versement des garanties lorsque les conditions convenues sont remplies. Ils ne couvrent que les éléments opérationnels du contrat hors ligne.

Au-delà de la nécessité de cadres juridiques, des normes convenues au niveau mondial assurant, entre autres choses, l'interopérabilité, devront être élaborées pour que l'on puisse commencer à utiliser la technologie à grande échelle. Une limitation essentielle des applications actuelles centrées sur la banque est le fait qu'elles peuvent traiter uniquement les transactions entre banques participant au projet. Un système véritablement mondial devrait connecter toutes les banques – ce qui représente un effort considérable et une tâche difficile sur le plan technique – ou alors il conviendrait de créer des passerelles entre les plates-formes existantes. Des efforts sont actuellement déployés pour traiter les questions juridiques et d'interopérabilité et élaborer des normes communes, mais il est probable que cela prendra du temps (voir la section 4.2 c)).

Troisièmement, il est possible que ces efforts eux-mêmes ne soient pas suffisants, comme le montre le cas des OBP. Bien que l'ICC ait élaboré des règles uniformes relatives aux OBP (URBPO), les entreprises ne se sont pas montrées très enthousiastes à l'idée d'utiliser les OBP. En définitive, le succès de la chaîne de blocs en matière de financement du commerce dépendra de la question de savoir si les entreprises voient de la valeur dans cette solution. Tout dépendra dans quelle mesure les avantages que la technologie peut rapporter dépassent les coûts de l'adaptation des systèmes actuels. Au-delà des questions juridiques et d'interopérabilité, cela ne pourra être le cas que si le commerce sous-jacent a été numérisé pour permettre la création de synergies et l'utilisation du plein potentiel de la chaîne de blocs

– c'est-à-dire si les différents aspects d'une transaction commerciale internationale, y compris les procédures douanières et la logistique, sont numérisés. À la différence des tentatives précédentes de numérisation du financement du commerce, les solutions basées sur la chaîne de blocs sont conduites par un ensemble beaucoup plus vaste de parties prenantes, y compris des banques, des autorités douanières, des fournisseurs de services logistiques, des gouvernements et des organismes de réglementation. Cela pourrait conférer à la chaîne de blocs la dynamique nécessaire pour réussir à numériser le commerce là où d'autres innovations technologiques ont échoué; le temps le dira. Toutefois, dans un proche avenir, il est probable que les applications continueront d'avoir une portée limitée.

Les investissements dans cette technologie restent de l'ordre du pari à ce stade, mais le foisonnement d'activités autour de la chaîne de blocs et les possibilités que cette technologie pourrait potentiellement ouvrir en font un défi que de nombreux établissements financiers estiment important de relever, ne serait-ce que pour ne pas être marginalisés si les incertitudes juridiques et opérationnelles qui entourent encore la chaîne de blocs étaient levées. Si tel était le cas, le paysage du financement du commerce pourrait bien être très différent à l'avenir. Il est intéressant de noter que certains observateurs estiment que, même si la chaîne de blocs est étroitement liée aux questions financières depuis ses débuts, la technologie a une meilleure chance d'avoir d'abord un impact réel dans des domaines tels que la facilitation des échanges, domaine dans lequel la coordination de multiples acteurs demeure un obstacle réel, ou pour ce qui est des questions liées à la traçabilité (voir la section 4.2 a)).

(b) La facilitation des échanges en action

Au cours des dernières années, la facilitation des échanges est devenue l'un des éléments centraux de la politique commerciale, non sans raison : l'inefficacité d'un certain nombre de procédures à la frontière continue d'imposer des coûts notables aux entreprises – et, en fin de compte, aux consommateurs et à l'économie dans son ensemble. La chaîne de blocs est considérée par beaucoup comme une occasion de faciliter les procédures commerciales et d'accélérer la numérisation du commerce transfrontières.

Alors qu'en 2013 les droits de douane se sont élevés à 9% en moyenne (OMC, 2015a), selon une étude de l'OMC de 2015, les coûts du commerce peuvent être équivalents à un droit *ad valorem* de 134% sur un produit dans les pays à revenu élevé et à un droit de 219% dans les pays en développement (OMC, 2015c). Ces coûts sont en grande partie la conséquence des formalités administratives et du nombre d'organismes intervenant dans les procédures à la frontière, qui rendent les procédures douanières onéreuses. En effet, en dehors des services douaniers, une multitude d'organismes gouvernementaux chargés de la santé, de l'alimentation, de

la quarantaine, de la sécurité sanitaire et de la protection des consommateurs interviennent traditionnellement dans les procédures douanières. Selon une étude basée sur un sondage, le nombre médian d'organismes gouvernementaux intervenant directement dans les transactions transfrontières est de 15 et ce chiffre peut atteindre 30 dans certains cas (Choi, 2011). Le nombre d'acteurs impliqués conduit à des procédures administratives complexes et souvent redondantes. Il est donc essentiel de simplifier les formalités administratives et d'automatiser les procédures, ce qui explique l'importance croissante accordée aux mesures de facilitation des échanges – c'est-à-dire à la simplification des procédures d'importation, d'exportation et de transit – ce qui a conduit à la négociation de l'Accord de l'OMC sur la facilitation des échanges (AFE).

L'AFE, adopté à la neuvième Conférence ministérielle à Bali en décembre 2013 et entré en vigueur en février 2017, vise à faciliter la mainlevée et le dédouanement des marchandises, à améliorer la transparence, et à promouvoir la coopération entre les services des douanes et les autres autorités compétentes en matière de facilitation des échanges et de respect des procédures douanières, y compris par l'utilisation de moyens électroniques pour échanger des données et des documents relatifs aux transactions commerciales transfrontières.

Bien que la facilitation des échanges soit un problème qui concerne toutes les nations commerçantes, elle revêt une importance particulière pour les pays en développement. Ce sont eux qui devraient tirer le meilleur parti de procédures douanières plus efficaces. D'après les estimations de l'OMC, la pleine mise en œuvre de l'AFE pourrait réduire les coûts du commerce mondial de 14,3% en moyenne, les pays africains et les pays les moins avancés (PMA) étant ceux, selon les prévisions, qui bénéficieraient de la plus forte réduction moyenne des coûts du commerce. La mise en œuvre complète de l'AFE pourrait également réduire le délai d'importation moyen de 47% et le délai d'exportation de plus de 90% (OMC, 2015c). Pour chaque dollar d'aide versé en vue de soutenir la réforme en matière de facilitation des échanges dans les pays en développement, la Banque mondiale estime que les gains économiques peuvent aller jusqu'à 70 dollars EU.¹¹

Un certain nombre d'organisations gouvernementales, régionales et intergouvernementales travaillent activement à la mise en œuvre de mesures commerciales sans papier. Par exemple, l'Accord-cadre de la Commission économique et sociale des Nations Unies pour l'Asie et le Pacifique (CESAP) sur la facilitation du commerce transfrontières sans papier en Asie et dans le Pacifique, adopté en juin 2016, vise à faciliter un commerce transfrontières sans papier entre les États membres de la CESAP qui le souhaitent, en permettant la reconnaissance mutuelle transfrontières des données et des documents liés au commerce sous forme électronique et en fournissant un cadre intergouvernemental spécifique pour

l'élaboration de solutions juridiques et techniques. Le Centre des Nations Unies pour la facilitation du commerce et les transactions électroniques (CEFACT-ONU) a élaboré une série de 40 recommandations (CEE-ONU, 2017) pour simplifier, normaliser et harmoniser les procédures commerciales et les flux de renseignements, dont certains sont directement liés à l'utilisation de moyens électroniques et de normes de structure des données électroniques pour l'échange de renseignements. Le CEFACT-ONU élabore également la sémantique de base visant à rendre possible l'échange électronique de renseignements. Les Parties à la Convention internationale pour la protection des végétaux (CIPV), un accord multilatéral déposé auprès de l'Organisation des Nations Unies pour l'alimentation et l'agriculture (FAO) qui vise à préserver les végétaux en empêchant l'introduction et la dissémination d'organismes nuisibles pour les végétaux, a adopté une norme qui décrit les principes et les lignes directrices pour l'élaboration et la délivrance des certificats phytosanitaires électroniques. La CIPV, avec l'appui du Fonds pour l'application des normes et le développement du commerce (STDF), a récemment lancé un hub mondial, ePhyto, pour faciliter les échanges de certificats phytosanitaires électroniques (ePhyto), en particulier entre les pays en développement : une organisation nationale de protection des végétaux d'un pays exportateur peut envoyer, via un système sécurisé, un certificat ePhyto vers le hub, qui le transfère ensuite à la « messagerie électronique »¹² du pays importateur.

Un nombre croissant d'économies vont également au-delà des simples systèmes d'automatisation douanière, dont le premier a été le Système douanier automatisé (SYDONIA), à savoir le système de gestion douanière mis au point par la Conférence des Nations Unies sur le commerce et le développement (CNUCED), et s'orientent vers des plates-formes plus intégrées et plus sophistiquées, le guichet unique, c'est-à-dire un « système permettant aux opérateurs qui participent au commerce et au transport de communiquer des informations et documents normalisés à un seul point d'entrée afin de satisfaire à toutes les formalités requises en cas d'importation, d'exportation et de transit ».¹³ De telles initiatives intègrent de plus en plus les certificats électroniques, telles que le guichet unique de l'Association des Nations de l'Asie du Sud-Est (ASEAN), qui est convenu d'un protocole d'échange de certificats d'origine électroniques entre certains de ses États membres et étudie l'établissement d'un certificat phytosanitaire électronique. L'importance de l'établissement de guichets uniques a été soulignée dans l'AFE de l'OMC.¹⁴

Toutefois, il reste beaucoup à faire. Dans une étude récente, la CESAP estime que le taux moyen mondial de mise en œuvre des mesures en faveur d'un « commerce sans papier » s'élève à seulement 50% environ, et les mesures en faveur d'un commerce sans papier plus avancées telles que les guichets uniques électroniques, ainsi que la présentation de demandes électroniques et la délivrance électronique de certificats d'origine préférentiels, restent à un stade relativement précoce

(CESAP, 2017). Ces dernières mesures n'ont été mises en œuvre en totalité ou en partie que par à peine plus de 40% des économies. La mise en œuvre de mesures transfrontières sans papier est encore plus faible. Des mesures telles que les échanges électroniques de certificats sanitaires et phytosanitaires ont été intégralement ou partiellement mises en œuvre dans moins de 30% des économies étudiées, les pays développés faisant un peu mieux en moyenne que les économies en développement, à l'exception de l'Amérique latine et des Caraïbes, qui sont leaders sur plusieurs fronts.

La chaîne de blocs est considérée avec espoir par de nombreux acteurs du commerce international comme une nouvelle possibilité de faciliter davantage et de numériser les transactions commerciales internationales. Les transactions transfrontières impliquent des échanges de données et de documents entre deux grandes catégories d'acteurs : les entreprises, les importateurs, les exportateurs, les banques et les entreprises de transport et de logistique (B), ainsi que les autorités gouvernementales (G). Les guichets uniques électroniques sont de plus en plus utilisés pour faciliter les processus G2G au niveau national (c'est-à-dire les échanges entre organismes publics nationaux) et B2G, mais les processus G2G transfrontières restent complexes. La chaîne de blocs peut-elle faciliter ces processus, améliorer les interactions G2G transfrontières pour des questions telles que la certification sanitaire et phytosanitaire, et permettre de se rapprocher d'un commerce véritablement sans papier ? Bien que la technologie présente des caractéristiques intéressantes pour faciliter certains aspects liés aux procédures à la frontière, le passage à un système sans papier basé sur la chaîne de blocs véritablement mondial demandera plus que la seule technologie.

(i) La chaîne de blocs pourrait faciliter les procédures nationales G2G et certaines procédures B2G à la frontière

Parce qu'elle permet l'échange et le traitement de renseignements avec toutes les personnes autorisées en temps réel et d'une manière très sûre, ainsi que l'automatisation des processus grâce à l'utilisation des contrats intelligents, réduisant ainsi au minimum les coûts de coordination et les retards, la chaîne de blocs pourrait améliorer l'efficacité d'un certain nombre de processus B2G, améliorer la coopération interinstitutions au niveau national et contribuer à administrer les guichets uniques, dans les cas où il en existe, d'une manière plus efficace. En particulier, elle pourrait s'avérer utile en ce qui concerne les aspects suivants :

B2G et coordination nationale interinstitutions

Le caractère très sûr, décentralisé et distribué de la chaîne de blocs pourrait soutenir et renforcer l'échange de renseignements entre organismes gouvernementaux au

niveau national et offrir à ceux-ci de nouvelles possibilités de coopérer plus efficacement (OMD, 2017). La chaîne de blocs est particulièrement adaptée aux situations qui font intervenir de multiples acteurs. Dans un système traditionnel, la plupart des parties prenantes agissent de façon cloisonnée et séquentielle, les données (par exemple expéditeur, courtier à l'exportation, services des douanes du pays importateur, documents bancaires et de transport) sont conservées séparément, et n'importe quelle partie peut y apporter des ajouts ou des modifications, ce qui rend ces données susceptibles de fraude, tandis que dans un système basé sur la chaîne de blocs, tous les renseignements sont partagés sur une plate-forme commune et quasiment impossibles à modifier. Toutes les parties concernées agissent de manière pleinement transparente et en temps réel, et toutes les actions peuvent facilement être retracées. Dans les cas où des autorisations multiples sont requises pour exporter un produit, l'exportateur ne serait tenu de saisir les renseignements qu'une seule fois. Les données seraient alors utilisées par les organismes respectifs connectés à la plate-forme pour valider la transaction ou délivrer les documents pertinents.

La preuve de concept menée par IBM pour expédier des fleurs de Mombasa (Kenya), jusqu'à la coopérative de Royal Flora aux Pays-Bas illustre bien les avantages que peut procurer la technologie.¹⁵ L'exportation de fleurs depuis le port de Mombasa nécessite la signature de trois organismes différents et six documents décrivant l'origine, le traitement chimique administré et la qualité des marchandises, ainsi que les droits de douane. Le cultivateur kenyan, par l'intermédiaire de son téléphone mobile, envoie une liste de colisage qui devient visible par tous les participants au registre avec permission. Cette action initie un contrat intelligent qui déclenche un flux de travail en vue de l'approbation de l'exportation au sein des trois organismes qui doivent approuver cette dernière. À mesure que chaque organisme donne son consentement, le statut de l'exportation est actualisé en temps réel et les autres participants peuvent le voir. Simultanément, des renseignements sur l'inspection des fleurs, le scellement du conteneur réfrigéré, la collecte par le transporteur routier et l'approbation des services des douanes sont communiqués au port de Mombasa, ce qui permet à celui-ci de préparer l'expédition du conteneur. À tout moment et tout au long du processus, toutes les actions liées aux documents et aux marchandises sont enregistrées et partagées dans le registre avec permission et sont visibles par tous les participants autorisés en temps réel : documents qui ont été présentés, à quel moment et par qui ; endroit où se trouvent les fleurs et personne en leur possession ; étapes suivantes.

Certification et procédures de licences

Comme le montre l'exemple de Royal Flora, l'utilisation de la chaîne de blocs peut contribuer à simplifier le flux de travail lié à l'approbation des certificats. Des

certificats sanitaires et phytosanitaires, des certificats d'origine et des certificats d'évaluation de la conformité délivrés par les autorités de confiance sont couramment requis pour donner l'assurance à l'importateur ou aux autorités compétentes du pays d'importation que les marchandises exportées satisfont à certaines prescriptions.

Une autre caractéristique de la technologie qui pourrait présenter un intérêt en matière de certification est le fait que les transactions par une chaîne de blocs incluent une référence aux transactions précédentes (un «pointeur de hachage»). Dans le cas des certificats phytosanitaires, par exemple, les envois ne peuvent pas être fractionnés puis envoyés au titre d'un seul certificat. Les exportateurs qui souhaitent fractionner leur envoi doivent revenir vers l'organisme qui a délivré le certificat et demander un certificat de remplacement. Avec un système basé sur la chaîne de blocs qui relie les transactions aux transactions précédentes de manière sûre et fiable, on pourrait imaginer qu'une demande de certificat de remplacement ne serait plus nécessaire dans les cas où les marchandises sont envoyées vers la même destination¹⁶ – ce qui pourrait grandement faciliter la vie tant des négociants que des organismes de certification – sous réserve, bien entendu, que le cadre réglementaire puisse être ajusté pour rendre cela possible.

La chaîne de blocs peut également s'avérer intéressante pour administrer les licences d'importation et d'exportation plus efficacement. Ces permis sont normalement délivrés pour une période définie. Le fait de stocker une licence d'importation ou d'exportation sur une chaîne de blocs épargnerait à l'importateur ou à l'exportateur le souci d'avoir à conserver le permis en lieu sûr pour éviter de le perdre et permettrait aux autorités douanières de vérifier facilement l'authenticité et la validité du permis. L'utilisation de permis falsifiés ne serait plus possible.¹⁷ L'utilisation d'un contrat intelligent permettrait même aux parties d'aller un peu plus loin en rendant un permis d'importation/d'exportation invalide à l'expiration de sa période de validité, ce qui pourrait aider à lutter contre la fraude et éviter les situations telles que celle qu'ont connu les Philippines en 2016, lorsque le Département de l'agriculture a annulé et rappelé tous les permis d'importation concernant les produits carnés pour lutter contre la fraude à l'importation de viande, après avoir constaté que d'anciens permis étaient recyclés pour effectuer des importations de contrebande (Fortune, 2016).

Les applications de la chaîne de blocs sont également étudiées en relation avec les certificats d'origine. Après avoir racheté eCertify et TradeCert, deux des principaux fournisseurs de certificats d'origine électroniques (eCO), en mai 2018, la société essDOCS, exploitant d'une plate-forme dédiée au commerce sans papier, a dévoilé une solution de nouvelle génération en matière de certificats d'origines électroniques, appelée essCert. Parmi les nouvelles fonctionnalités offertes par essCert figurent

des options basées sur la chaîne de blocs/la technologie des registres distribués, qui permettent aux chambres de commerce de relier les données des certificats d'origine électroniques aux plates-formes de chaînes de blocs et aux appareils de l'Internet des objets (IdO) afin d'améliorer la vérification de l'origine (essDOCS, 2018).

Le même mois, la Chambre de commerce internationale de Singapour, qui est habilitée à délivrer des certificats d'origine, et la société de technologie financière vCargo Cloud ont dévoilé une plate-forme de chaînes de blocs avec permission dédiée aux certificats d'origine électroniques visant à améliorer l'efficacité, à réduire au minimum les coûts de la vérification des certificats d'origine et à prévenir la fraude. Le système fournit une solution hybride lorsque le destinataire n'est pas prêt à accepter des documents numériques. Dans ce cas, tant un exemplaire numérique qu'un exemplaire papier sont délivrés, et un code QR* contenant l'empreinte* de l'exemplaire numérique qui se trouve sur la chaîne de blocs est inséré sur l'exemplaire papier. Le code QR peut être numérisé à l'aide d'un smartphone pour vérifier le certificat d'origine électronique. Ces certificats d'origine électroniques peuvent être imprimés, mais le nombre d'impressions autorisées est limité afin d'empêcher les copies non autorisées (IT News Africa, 2018).

Le Kenya, la République de Corée et le Royaume-Uni travaillent sur des projets similaires, et le Marché commun de l'Afrique orientale et australe (COMESA) a annoncé en février 2018 un projet pilote utilisant la chaîne de blocs pour sa nouvelle zone de libre-échange numérique visant à connecter les parties à une transaction en temps réel grâce à une plate-forme de chaînes de blocs. Le système intégrera un certificat d'origine électronique (Mbogo, 2018).

Un point important à noter au sujet des certificats d'origine est que l'authentification par les chambres de commerce n'atteste pas de la véritable origine du produit, seulement de la déclaration fournie aux chambres de commerce par l'exportateur, ce qui amène certains à faire valoir que, en réalité, une telle authentification ne serait pas véritablement nécessaire. La chaîne de blocs ne modifierait pas cet état de fait. D'une certaine façon, les avantages que procurent un système basé sur la chaîne de blocs dans le cadre de la délivrance de certificats d'origine se limiteraient à la possibilité de prouver que le certificat est authentique – c'est-à-dire qu'il a bien été délivré par l'autorité compétente – et qu'il n'a pas été falsifié. Toutefois, si les utilisations de la chaîne de blocs dans le domaine de la traçabilité se développent plus largement (voir la section 4.2 a)), on pourrait imaginer qu'un jour la certification de l'origine s'appuierait sur les données de la chaîne de blocs pour être déterminée directement à la frontière, sans qu'une autorité de certification soit nécessaire. L'annonce par le Bureau des douanes et de la protection des frontières des États-Unis, en août 2018, qu'il allait lancer un test afin de suivre les renseignements

et d'aider à confirmer que les produits importés depuis le territoire de partenaires de l'Accord de libre-échange nord-américain et de l'Accord de libre-échange d'Amérique centrale sont bien originaires de l'endroit allégué, pourrait être une première étape en ce sens (Baydakova, 2018).

Mainlevée et dédouanement des marchandises

Les applications de la chaîne de blocs pourraient améliorer l'efficacité des processus de dédouanement et réduire la nécessité d'une vérification manuelle. En particulier, la chaîne de blocs pourrait être utilisée dans les cas suivants :

- pour présenter des demandes de décisions anticipées.¹⁸ Les décisions, une fois rendues, seraient stockées en sécurité sur la chaîne de blocs, dans un registre avec permission, et resteraient accessibles à tout moment par les parties prenantes autorisées, y compris tous les bureaux des douanes situés sur le territoire, pendant toute la durée de validité de la décision, ce qui faciliterait le processus de mainlevée et de dédouanement;
- pour faciliter le traitement avant arrivée¹⁹, c'est-à-dire le traitement avant l'arrivée des marchandises et la mainlevée accélérée des marchandises²⁰, puisque les données requises peuvent être partagées dans le registre en temps réel;
- pour optimiser l'évaluation des risques.²¹ À mesure que les documents douaniers sont présentés via le système, ils seraient immédiatement et automatiquement analysés et évalués sur la base de critères de sélection prédéterminés codés dans un contrat intelligent. Les envois répondant aux critères de sélection seraient automatiquement signalés;

Le potentiel de la technologie dans ces différents domaines n'a pas encore été pleinement examiné, mais certaines initiatives voient le jour. En mai 2018, les Services coréens des douanes, par exemple, ont annoncé le développement d'une plate-forme douanière basée sur la chaîne de blocs pour faciliter le dédouanement des produits vendus en ligne. Les autorités douanières de la République de Corée ont signé un mémorandum d'accord avec des sociétés de commerce électronique afin de mener des essais utilisant la technologie de chaînes de blocs en vue d'accélérer le dédouanement des produits vendus en ligne par lesdites sociétés, de partager les renseignements en temps réel, de générer un rapport de dédouanement à l'importation automatisé à l'intention des autorités et de prévenir la fraude et la contrebande (CCN, 2018).

Admission temporaire des marchandises

Les marchandises importées dans un but spécifique et pour une période limitée, telles que des tableaux pour une exposition, sont admises en suspension des droits et taxes à l'importation, à la condition d'être réexportées dans un délai déterminé sans avoir subi de modification (exception faite de leur dépréciation normale).²²

L'utilisation de la chaîne de blocs pour suivre leurs déplacements et partager les renseignements pourrait permettre de se passer des processus actuels qui nécessitent beaucoup de papier et d'améliorer l'efficacité de la procédure d'admission temporaire.

Une preuve de concept menée par la DG TAXUD²³ de la Commission de l'UE en coopération avec la Chambre de commerce internationale a démontré que la chaîne de blocs pourrait être utilisée pour garantir l'intégrité des carnets d'admission temporaire (également appelés carnets ATA)²⁴ et des transactions. Un projet pilote va maintenant être lancé pour tester l'application (Saadaoui, 2018).

Recouvrement des recettes et exactitude des données commerciales

Les contrats intelligents pourraient être codés sur la base des prescriptions légales et réglementaires pour permettre le paiement automatique des droits de douane selon la formule « si... alors », par exemple, si les marchandises arrivent au terminal douanier en vue d'être importées, « alors » le paiement des droits intervient automatiquement. Un mécanisme numérique permettant de suivre les événements extérieurs, également connu sous le nom d'oracle*, pourrait être utilisé pour déclencher l'exécution de contrats intelligents lorsque des conditions prédéfinies sont remplies, ce qui remplacerait l'autodéclaration. Ainsi, un oracle pourrait être programmé pour suivre un camion équipé de capteurs et déclencher le paiement des droits lorsque le camion franchi la frontière.

Les applications de la chaîne de blocs pourraient aussi permettre aux intermédiaires de recouvrer les droits et les taxes au nom des gouvernements et de les transférer automatiquement aux autorités respectives en utilisant des contrats intelligents – ce qui s'avèrerait utile dans le cas d'envois de faible valeur liés, par exemple, au commerce électronique.

Enfin, l'utilisation de la chaîne de blocs pour enregistrer les droits de douane imposés sur les importations pourrait contribuer à améliorer l'exactitude des données et des statistiques commerciales.

Contrôle après dédouanement²⁵

Comme dans le cas de la gestion des risques, les contrats intelligents pourraient être utilisés pour examiner les documents sur la base de critères prédéfinis afin d'optimiser le contrôle après dédouanement. En cas de doute, le caractère immuable de la chaîne de blocs fait qu'il est possible de suivre et de vérifier facilement les transactions.

Gestion du respect des règles

Grâce à la chaîne de blocs, il pourrait être plus facile de déterminer la provenance des produits – et, donc, par exemple, de prouver le respect des dispositions relatives au traitement préférentiel accordé dans le cadre d'accords de libre-échange – et de contribuer à réduire la fraude, les inexactitudes et les erreurs (voir la section 4.2 a)).

Gestion des identités

La chaîne de blocs pourrait faciliter la vérification des identités des entreprises et des personnes, y compris des opérateurs économiques agréés (OEA).²⁶

La capacité de la chaîne de blocs d'améliorer l'efficacité des procédures à la frontière et des transactions B2G au niveau national est multiforme. Diverses organisations, telles que la CEFAC-ONU, la Convention internationale sur le commerce des espèces de faune et de flore sauvages menacées d'extinction (CITES) et l'Organisation mondiale des douanes (OMD) examinent de quelle manière la technologie pourrait être mise en œuvre et intégrée aux systèmes douaniers et aux processus de certification existants, tandis que des sociétés informatiques et des organismes gouvernementaux s'associent pour étudier le potentiel de la technologie en mettant au point des preuves de concept et des projets pilotes. Toutefois, même si la chaîne de blocs peut fournir un outil pour administrer les procédures à la frontière et les guichets uniques au niveau national d'une manière plus efficace, plus transparente et plus sûre, le véritable défi sera de rendre les processus G2G plus efficaces.

(ii) L'espoir de processus transfrontières G2G facilités

Les transactions électroniques transfrontières B2B sont courantes et ont sous-tendu la mondialisation économique depuis l'essor d'Internet, mais les échanges électroniques transfrontières G2G qui appuient les chaînes d'approvisionnement en sont encore à leurs balbutiements (Stokes, 2017). Le caractère décentralisé de la chaîne de blocs est vu avec espoir par de nombreux acteurs du domaine comme une occasion de contribuer à surmonter certains défis qui rendent les processus transfrontières G2G complexes ou risqués.

La technologie pourrait s'avérer intéressante, par exemple, pour atténuer les risques associés à certains types de processus transfrontières G2G, tels que le partage de renseignements liés aux opérateurs économiques agréés. La mise en œuvre des accords de reconnaissance mutuelle (ARM) des OEA se heurte à de nombreux défis, y compris le traitement manuel de données sensibles et/ou confidentielles avec des critères de sécurité et d'intégrité peu élevés, la difficulté d'établir la provenance et la traçabilité des données et de garantir un accès sécurisé,

l'incapacité d'accorder des avantages aux OEA en temps réel et l'incapacité de réagir en temps réel lorsqu'une suspension intervient, avec toutes les conséquences que cela peut entraîner pour la sécurité de la chaîne d'approvisionnement (Corcuera-Santamaria, 2018). Les caractéristiques spécifiques de la technologie pourrait améliorer la gestion transfrontières des ARM en rendant possible l'automatisation du processus de partage des données relatives aux OEA entre les parties à un ARM en temps réel et de manière sécurisée, et en fournissant un mécanisme traçable qui garantit l'intégrité des données. La capacité de la technologie de faciliter la mise en œuvre des accords de reconnaissance mutuelle des OEA est actuellement examinée. Un projet pilote entre le Mexique et le Costa Rica (appelé Cadena) a été lancé en mars 2018 avec le soutien de la Banque interaméricaine de développement afin de créer une plate-forme commune pour la gestion des OEA.

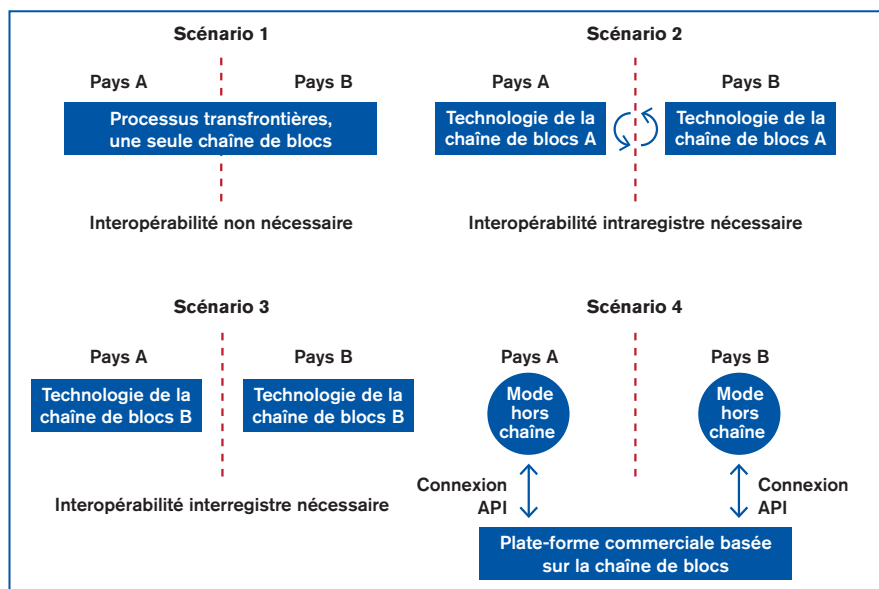
La technologie peut-elle faciliter les différentes dimensions des interactions transfrontières G2G intervenant lors du dédouanement des marchandises, en particulier les échanges G2G de documents douaniers et de certificats ? Les défis liés aux processus transfrontières G2G sont, d'une manière générale, de trois types : l'interopérabilité technique, qui permet à des systèmes informatiques de communiquer entre eux au niveau technique, les questions réglementaires et la simplification et la standardisation des données. Alors que la chaîne de blocs pourrait apporter une aide pour ce qui est du premier point – dans certaines conditions – elle ne peut pas faire grand-chose en ce qui concerne les questions réglementaires. En fait, ces dernières détermineront dans une large mesure la capacité de la chaîne de blocs d'améliorer véritablement les processus G2G.

(iii) Interopérabilité technique

Le passage à des documents numériques, tels que les certificats phytosanitaires électroniques, a soulevé de nouvelles questions d'interopérabilité. Dans le monde du papier, ces documents sont simplement présentés sur papier aux autorités compétentes. Le passage aux documents numériques nécessite l'établissement de « passerelles électroniques » *ad hoc* entre les autorités compétentes des pays importateurs et exportateurs, ce qui peut être un processus complexe et fastidieux. La création de hubs, tels que le hub e-Phyto lancé récemment par la CIPV, peut aider à gérer l'acheminement des connexions, mais ces hubs ne fournissent pas une approche holistique, intégrée – sans oublier qu'ils peuvent soulever des problèmes en termes d'administration (par exemple nécessité de faire confiance à une tierce partie), de conséquences financières liées à la gestion du hub, et de sécurité (par exemple point de défaillance unique).

La chaîne de blocs peut-elle faciliter des processus G2G d'un point de vue technique ? La réponse n'est pas simple. Cela dépend beaucoup de l'environnement technique effectif au niveau national à la fois du côté de l'importateur et du côté de l'exportateur. Le scénario idéal voudrait que les autorités gouvernementales importatrices et exportatrices fassent partie de la même chaîne de blocs unique. Dans ce cas, aucune interopérabilité ne serait nécessaire. Les données pourraient être échangées directement entre une partie et une autre par l'intermédiaire de la plate-forme, sur la base des règles de la plate-forme (voir la figure 9, scénario n° 1). Les contrats intelligents pourraient être codés de façon à partager seulement certains types de données avec d'autres autorités gouvernementales et d'autres participants à la plate-forme. Ce scénario, qui est le plus ambitieux, donne lieu à des essais de la part de divers acteurs sur le terrain. L'un de ces projets est l'initiative de la déclaration en douane à Singapour («Singapore Customs Declaration»). En collaboration avec les services singapouriens des douanes, IBM a mis au point un portail douanier basé sur la chaîne de blocs qui lui permet d'envoyer des déclarations en douane depuis New York jusqu'à Singapour.²⁷ Un registre avec permission permet à tous les membres du réseau d'accéder aux renseignements douaniers stockés à un seul endroit et ce, en temps réel. Divers consortiums du secteur privé dans le domaine du transport et de la logistique examinent également la possibilité de mettre au point des plates-formes commerciales multipartites (voir la section 3.1 c)). Bien que, en théorie, ces plates-formes seraient idéales, il est difficile d'envisager un tel scénario à l'échelle mondiale. Il est plus probable que cette approche sera limitée à certaines lignes commerciales et certaines autorités douanières, différentes plates-formes fonctionnant en parallèle.

Un autre scénario serait celui où les autorités gouvernementales, tant du côté des importateurs que des exportateurs, participeraient à deux plates-formes différentes construites à partir de la même technologie de chaîne de blocs (par exemple Hyperledger Fabric). Dans ce cas, l'«interopérabilité intraregistre» – c'est-à-dire l'interopérabilité entre des plates-formes de chaîne de blocs construites à partir de la même technologie de chaîne de blocs – serait nécessaire (voir la figure 9, scénario n° 2). Cette interopérabilité fait l'objet de recherches intensives et des solutions commencent à émerger. Par exemple, en mai 2018, l'Enterprise Ethereum Alliance, a dévoilé un cadre libre multi-plates-formes fondé sur des normes pour les chaînes de blocs avec permission basées sur l'Ethereum qui permettrait l'interopérabilité entre les chaînes de blocs avec permission construites à partir de la chaîne de blocs publique Ethereum (Higgins, 2018). Comme dans les scénarios n° 1 et n° 3 de la figure 9, les contrats intelligents garantiraient que seuls certains types de renseignements peuvent être extraits par les autres autorités pertinentes. Compte tenu des multiples protocoles de chaînes de blocs qui voient le jour, il est probable qu'un tel scénario serait limité à quelques cas seulement.

Figure 9 Scénarios des processus G2G transfrontières

Source: Auteure.

Les scénarios n° 3 et 4 de la figure 9 ont davantage de chances de devenir réalité dans les années à venir. Dans le scénario n° 3, les autorités gouvernementales situées de chaque côté de la transaction participeraient chacune à une plate-forme différente, basée sur sa propre technologie. Dans ce cas, une interopérabilité inter-registres serait nécessaire. Consciente des enjeux, la communauté de la chaîne de blocs recherche activement des solutions possibles. Des outils d'interopérabilité entre Hyperledger et Ethereum, par exemple, sont en cours d'élaboration.²⁸ Une autre approche, plus globale, qui est à l'étude, consisterait à créer un système de notariation inter-registres qui permettrait aux parties autorisées de vérifier les transactions quel que soit le registre sur lequel elles sont créées (CEFACT-ONU, 2018). La notariation pourrait être réalisée par une seule entité ou plusieurs – ce qui toutefois, nécessiterait la réintroduction d'un certain degré de centralisation. Au sein de la communauté, nombreux sont ceux qui considèrent le développement d'un système de notariation comme un élément crucial d'une interopérabilité à large échelle (voir aussi la section 4.2 a)).

Dans le scénario n° 4, certaines autorités gouvernementales des pays importateurs et exportateurs, voire toutes, resteraient hors-chaîne et interagiraient avec une plate-forme commerciale donnée basée sur la chaîne de blocs via des interfaces de programmation applicatives ou API (c'est-à-dire des interfaces permettant d'extraire des renseignements d'un système pour les transférer vers un autre) au cas par cas

– sous réserve que le codage utilisé par les contrats intelligents de la chaîne de blocs soit compatible avec les API. Dans ce scénario, la chaîne de blocs ne ferait rien pour faciliter l'interaction transfrontières G2G, qui continuerait de se dérouler comme avant l'introduction du nouveau système de la chaîne de blocs. Un tel scénario pourrait néanmoins présenter une certaine valeur à la fois pour les organismes gouvernementaux et pour les participants à la plate-forme commerciale basée sur la chaîne de blocs: les API pourraient permettre aux organismes gouvernementaux d'extraire les renseignements pertinents de la plate-forme pour accélérer le dédouanement et d'autres processus, et les participants à la chaîne de blocs seraient en mesure d'obtenir les renseignements autorisés auprès des organismes gouvernementaux afin de faciliter les processus qu'ils gèrent via la plate-forme.

Ces différents scénarios montrent que, si la chaîne de blocs peut, dans un système intégré, faciliter considérablement l'interaction G2G transfrontières, ce ne sera probablement pas la panacée pour résoudre les problèmes d'interopérabilité G2G au niveau mondial. Un système intégré véritablement mondial est peu probable. Un scénario plus plausible est celui de la coexistence au niveau mondial de plusieurs plates-formes construites à partir de technologies différentes. À moins que les problèmes d'interopérabilité entre ces plates-formes ne soient résolus, il est peu probable que l'utilisation de la chaîne de blocs pour faciliter l'interaction technique transfrontières G2G et, plus généralement, les transactions commerciales internationales fasse réellement la différence.

(iv) Questions réglementaires

Le passage à un système sans papier demande plus que la technologie et l'interopérabilité technique. Il nécessite un cadre réglementaire propice, qui prévoit des méthodes d'authentification électronique ainsi que la reconnaissance des signatures électroniques, des documents électroniques et des transactions électroniques; qui reconnaît le pouvoir des autres entités gouvernementales (à la fois nationales et étrangères) de délivrer les documents nécessaires, tels que les certificats; et qui permet le partage de certains types de renseignements entre autorités gouvernementales. Cela est vrai au niveau national, où de nombreux échanges électroniques entre un organisme et un autre ne peuvent avoir lieu parce que le cadre approprié n'a pas été mis en place, mais encore plus au niveau international.

Examiner la législation nationale dans son ensemble et l'adapter pour donner une reconnaissance légale aux signatures électroniques et aux documents électroniques peut être nécessaire. À ce jour, seul un nombre limité de pays ont des dispositions légales permettant cette reconnaissance. La plupart des pays – ainsi que les

acheteurs commerciaux/les importateurs – continuent de demander des versions papier des documents. En outre, dans de nombreux pays, la législation nationale doit être adaptée pour autoriser l'accès et le partage de renseignements avec une autre administration, même au niveau national. Une première étape devrait consister à reconnaître les signatures électroniques et les transactions électroniques à l'échelle nationale, et à envisager ensuite d'accepter ce type de messages de la part des autres pays. La reconnaissance des documents électroniques délivrés par une entité d'un autre pays nécessite des accords au cas par cas (UNNExT, CEE-ONU, CESAP-ONU, 2012).

À ce jour, il n'existe que quelques circuits d'échange véritablement sans papier, tels que celui d'échange de certificats sanitaires entre les Pays-Bas et la Chine pour les produits laitiers et d'échange de certificats phytosanitaires entre les Pays-Bas et la Colombie pour les fleurs.²⁹ L'établissement de circuits de ce type est complexe et chronophage, notamment parce que les questions réglementaires doivent être résolues produit par produit.

Le passage à la chaîne de blocs nécessiterait encore de définir les paramètres réglementaires qui permettent que les données soient échangées entre les autorités compétentes. La technologie peut être nouvelle, mais les mêmes obstacles réglementaires subsistent. Toutefois, les caractéristiques intrinsèques de la chaîne de blocs et la possibilité d'utiliser des contrats intelligents pour limiter l'accès aux renseignements uniquement aux personnes autorisées pourraient potentiellement faciliter l'établissement de ces circuits en créant un environnement sûr et de confiance pour l'échange de données – sous réserve de la volonté politique nécessaire.

Si la chaîne de blocs peut contribuer à accélérer la numérisation du commerce et à améliorer l'efficacité des procédures à la frontière, le chemin à parcourir pour parvenir à un commerce véritablement sans papier est encore long. Un soutien politique de haut niveau est nécessaire pour mener l'intégration du commerce et aider à établir un cadre juridique propice à un commerce sans papier. En fait, l'un des obstacles à une plus grande intégration du commerce pourrait être d'ordre politique. Aujourd'hui, seuls un nombre limité de guichets uniques dans le monde sont pleinement intégrés. Nombre d'entre eux sont construits sur des interfaces qui permettent l'échange électronique de renseignements, mais pas le traitement des données.³⁰ L'une des raisons est la réticence des autorités à partager des données via des moyens électroniques avec d'autres autorités. Le niveau de sécurité plus élevé qu'offre la chaîne de blocs permettra-t-il de changer la donne ? L'avenir le dira.

(v) Simplification et normalisation des données

En outre, la chaîne de blocs ne pourra fonctionner à son plein potentiel que si les données sont introduites dans un format qui permet aux divers participants de les comprendre de la même manière et de les traiter facilement en tant que parties du système. Il est crucial d'harmoniser la sémantique (c'est-à-dire le sens des renseignements échangés). Tant la CEFACT-ONU que l'OMD ont élaboré des bibliothèques sémantiques (voir également la section 4.2 b)). L'élaboration d'ensembles de données normalisés qui recouvrent toutes les données utilisées pour l'échange de renseignements concernant l'importation, l'exportation, le transit – et idéalement, les modes de transport et la finance – et l'harmonisation des processus sont également essentiels.³¹ La CIPV a publié un format standard pour les certificats phytosanitaires électroniques, mais ce n'est pas le cas pour les autres documents requis pour les transactions commerciales transfrontières, tels que les certificats vétérinaires, par exemple, qui restent bilatéraux. La chaîne de blocs peut potentiellement améliorer les procédures commerciales transfrontières, mais elle ne pourra pas résoudre les questions de normalisation. La mise en œuvre d'une plate-forme de chaînes de blocs sans avoir rationalisé les processus ni harmonisé la sémantique en amont irait à l'encontre même de l'objectif d'un système basé sur la chaîne de blocs. S'agissant des certificats vétérinaires, des travaux sont en cours au Codex Alimentarius³² et à l'Organisation mondiale de la santé animale (OIE) en vue d'élaborer un format standard pour les certificats vétérinaires, mais il faudra probablement un certain temps avant qu'une norme de ce type ne soit convenue.³³

L'élaboration de normes uniques est un processus lent et fastidieux. Une approche plus flexible pourrait consister à répertorier les formats existants et les façons d'introduire les données, et de convenir d'un ensemble d'approches qui permettraient de faire en sorte que des contrats intelligents perfectionnés soient codés de façon à extraire les données requises et à les traiter via une plate-forme de chaîne de blocs. L'apprentissage automatique et l'intelligence artificielle pourraient être des outils utiles à cet égard. Au lieu d'harmoniser les approches en amont, avec le risque que les normes uniques convenues puissent rapidement devenir obsolètes, cette approche s'appuierait sur la «standardisation de la diversité»: la diversité des approches serait reconnue et répertoriée, dans l'intention de fournir un «menu de manières «standard»» d'introduire les données. Le commerce intelligent demande une normalisation, mais il a besoin d'une normalisation intelligente et flexible.

Enfin, dernier point, mais non le moindre, des procédures transfrontières efficaces ne dépendent pas seulement d'organismes gouvernementaux bien coordonnés. Elles demandent aussi une intégration efficace des divers aspects d'une transaction commerciale transfrontières, du financement du commerce aux formalités douanières, en passant par la logistique. Sur ce front également, la situation évolue rapidement.

(c) Combiner le tout : le pari des sociétés de transport et de logistique

Le transport et la logistique sont la colonne vertébrale du commerce international. Le secteur constitue un terrain fertile pour la mise en œuvre de la chaîne de blocs en raison du nombre élevé d'acteurs impliqués. Il n'est pas surprenant que les ports, ainsi que les sociétés de transport et de logistique étudient activement le potentiel de la chaîne de blocs, en combinaison avec l'Internet des objets, dans l'espoir d'abaisser les coûts et d'améliorer les processus, et pour certains, avec l'ambition déclarée d'établir des plates-formes commerciales qui pourraient relier tous les acteurs le long de la chaîne d'approvisionnement, des expéditeurs aux autorités douanières en passant par les banques, pour tenter de numériser le commerce international. Le développement de plates-formes de ce type pourrait non seulement avoir une influence notable sur le secteur du transport et de la logistique lui-même, mais aussi transformer profondément le commerce international des marchandises.

Cette technologie présente sans aucun doute des avantages potentiels très larges pour le secteur du transport et de la logistique, tels que l'aide au suivi des navires et des camions, l'optimisation des capacités de chargement, la réduction des coûts administratifs et de coordination, l'accroissement de la transparence en matière de prix, de propriété et en ce qui concerne l'ensemble de la chaîne de transport, l'accélération des paiements grâce à l'utilisation des contrats intelligents, l'amélioration de la sécurité et la réduction de la fraude, ainsi que la simplification de la liquidation des sinistres en créant un registre immuable des antécédents de transport. Les expéditions internationales sont généralement gérées par diverses entreprises en cours de route. Le fait que tous les renseignements pertinents concernant l'expédition soient partagés avec les partenaires autorisés en temps réel sur une chaîne de blocs sécurisée garantissant que toute donnée quelconque ajoutée n'a pas été falsifiée peut considérablement améliorer la coordination, accélérer les processus et réduire les coûts. L'un des avantages majeurs que la chaîne de blocs offre en matière de transport et de logistique est la possibilité de renforcer la collaboration entre les différentes entreprises participantes, tout en leur permettant de garder le contrôle des renseignements sensibles et de décider qui sait quoi et à quel moment.

Ces avantages potentiels conduisent un nombre croissant d'entreprises du secteur à mettre au point des applications de la chaîne de blocs. La société de transport et de logistique Nippon Yusen Kabushiki Kaisha (NYK), par exemple, participe à un consortium en vue d'élaborer une plate-forme de partage de données commerciales basée sur la chaîne de blocs qui vise à améliorer la logistique de sa chaîne d'approvisionnement. Le consortium, formé par NTT Data Corporation Japon, comprend 14 sociétés de divers secteurs participant au commerce international, y compris du secteur bancaire, du secteur des assurances, de celui de la logistique

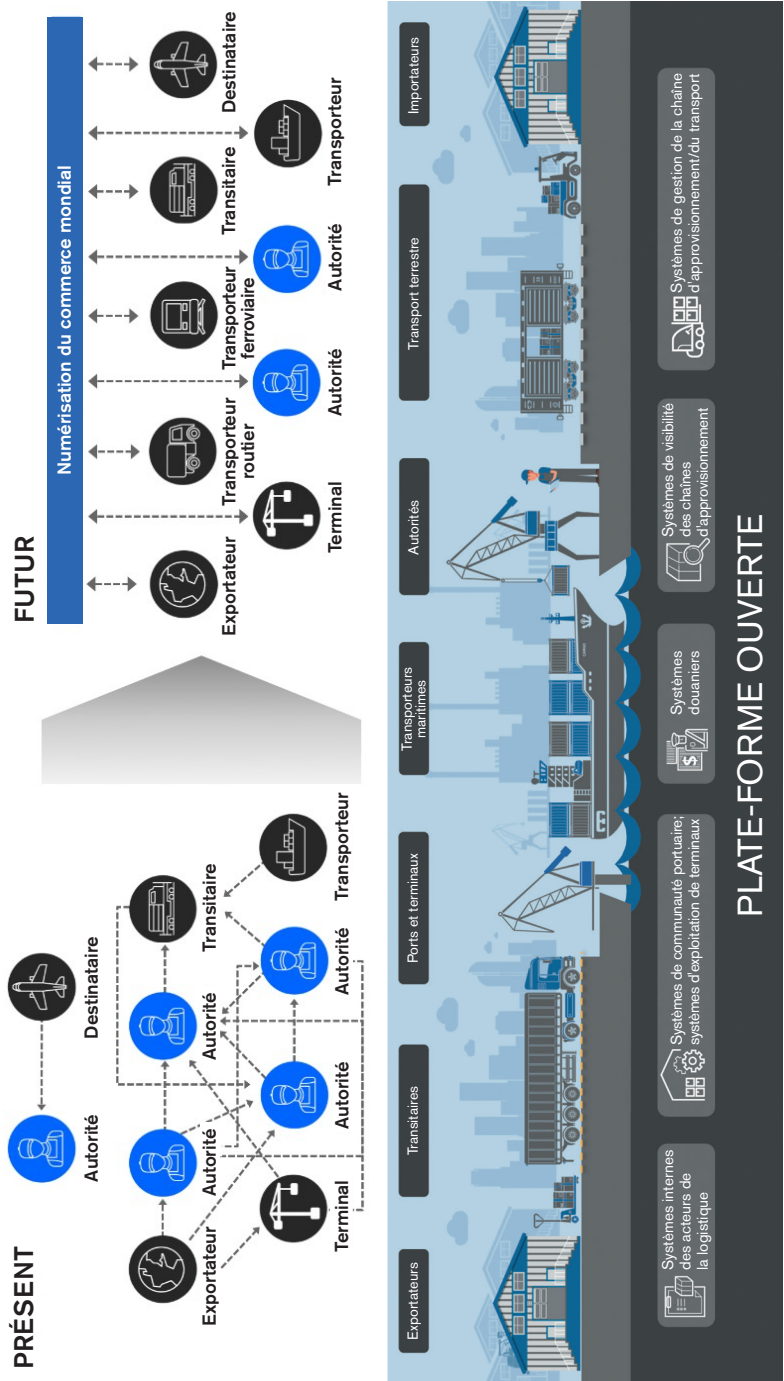
intégrée, ou encore de l'import-export. Un autre exemple est Marine Transport International (MTI), un transitaire basé au Royaume-Uni et aux États-Unis, qui a mené à bien un projet pilote portant sur son système de chaîne de blocs publique Container Streams. D'après la société MTI, le projet a démontré que le secteur de la logistique bénéficierait d'une connectivité, d'une efficacité et d'une sécurité améliorées grâce à la chaîne de blocs (Marine Transport International (MTI), 2017). En République de Corée, Hyundai Merchant Marine a mené en 2017 plusieurs essais grandeur nature portant sur un système mis au point par Samsung. D'autres initiatives comprennent Blockfreight³⁴, un projet de SAP³⁵ pour le transport maritime et Quasa³⁶, une plate-forme de chaîne de blocs ouverte pour les sociétés de transport en Russie et dans la Communauté d'États indépendants. Ce ne sont que quelques-uns des projets élaborés dans ce domaine.

Le nombre de projets de ports intelligents ayant une composante « chaîne de blocs » s'accroît également rapidement. En Europe seulement, des ports tels que Hambourg, Anvers et Rotterdam examinent tous la capacité de la chaîne de blocs de les aider à simplifier leurs activités et à améliorer le partage des renseignements logistiques et contractuels entre les parties.

Les initiatives se multiplient aux quatre coins du monde, ce qui conduit certains observateurs à dire que la chaîne de blocs est sur le point de révolutionner le monde du transport et de la logistique.³⁷ Certains projets en cours d'élaboration pourraient, en fait, avoir un impact encore plus large. Les tentatives de certaines sociétés de travailler avec les autorités gouvernementales en vue de mettre au point des plates-formes qui connecteraient tous les acteurs le long de la chaîne d'approvisionnement pourraient être révolutionnaires – mais ce n'est pas sans défis.

Avec 90% des marchandises échangées au niveau international transportées par mer, le transport maritime joue un rôle crucial dans le commerce mondial. L'un des principaux acteurs du secteur, Maersk, a travaillé activement avec IBM afin d'élaborer une plate-forme commerciale mondiale basée sur la chaîne de blocs, appelée TradeLens³⁸, qui vise à connecter les diverses parties participant au commerce international – des transitaires aux autorités gouvernementales – et à numériser la chaîne d'approvisionnement du début à la fin, en vue de simplifier et de faciliter les procédures (voir la figure 10). La plate-forme a été officiellement lancée en août 2018 après avoir été mise à l'essai pendant plusieurs mois (Wass, 2018b). Un conseil consultatif intersectoriel sera établi afin de prendre en considération les besoins spécifiques des divers secteurs concernés par la conception de la plate-forme dans le but d'élaborer une plate-forme pour la branche d'activité tout entière. Le module pour les documents commerciaux, appelé ClearWay, permet aux importateurs, aux exportateurs, aux courtiers en douane et aux tierces parties de confiance, telles que les services des douanes et autres organismes

Figure 10 Projet de numérisation du commerce mondial Maersk-IBM



Source : White, M. (2018).

gouvernementaux, de collaborer en matière de processus opérationnels interorganismes, et permet l'automatisation de divers processus opérationnels tels que le dédouanement à l'importation et à l'exportation via des contrats intelligents. Le succès de la plate-forme dépendra en définitive de son adoption, ou non, par les différents acteurs participant au commerce international. Au moment de son lancement, plus de 20 exploitants de ports et de terminaux du monde entier, représentant plus de 230 portes d'entrées maritimes, ainsi que 2 autres transporteurs maritimes (Pacific International Lines et Hamburg Süd), plusieurs transitaires et courtiers en douane, ainsi que des autorités douanières en Arabie saoudite, en Australie, aux Pays-Bas, au Pérou et à Singapour, participaient déjà ou avaient annoncé qu'ils allaient participer à la plate-forme.³⁹ C'est là un début prometteur. Toutefois, aucune banque ne fait partie du projet à ce stade, et la plate-forme TradeLens n'est pas la seule de ce type.

D'autres sociétés, y compris des concurrents de Maersk, étudient des approches de bout-en-bout similaires. Après avoir réalisé avec succès une preuve de concept au début de l'année 2018 afin de numériser les connaissements en coopération avec APL Ltd. (qui est détenue par le troisième plus grand transporteur par conteneur du monde), la société logistique Kuehne + Nagel, et les services danois des douanes (The Maritime Executive, 2018), Accenture, par exemple, envisage d'élargir l'essai à des acteurs clés tant du côté de l'importateur que de l'exportateur, y compris à des autorités douanières à l'exportation et des banques (voir la figure 3).

Si ces projets réussissent, la chaîne de blocs pourrait bien devenir l'avenir de l'infrastructure commerciale et le plus grand facteur de disruption du secteur du transport et du commerce international depuis l'invention du conteneur. Toutefois, il reste plusieurs défis à relever.

Premièrement, les plates-formes commerciales mondiales ne peuvent livrer tout leur potentiel qu'une fois que les échanges sous-jacents ont été numérisés, y compris les processus de financement du commerce et de dédouanement, ainsi que les documents clés tels que les connaissements (c'est-à-dire la liste détaillée de la cargaison d'un navire remise par le capitaine du navire à la personne expédiant les marchandises). Comme cela a été indiqué dans les sections précédentes, la numérisation complète des procédures douanières et de financement du commerce n'est pas encore une réalité. Pour ce qui est des documents clés tels que les connaissements, des projets examinant de quelle façon la chaîne de blocs pourrait être exploitée pour les numériser sont en cours. De précédentes tentatives visant à créer des systèmes de connaissements électroniques, tels que SEADOCS, ont échoué et ces systèmes n'existent plus, principalement du fait de la nécessité de s'abonner au système. Toutefois, parce que la chaîne de blocs rend possible la réalisation des transactions de pair à pair, sans qu'un abonnement préalable ne soit

nécessaire, elle ouvre de nouvelles perspectives dans ce domaine. D'après Accenture, l'utilisation de la chaîne de blocs a conduit à une réduction de 80% des efforts associés à la gestion des données relatives au connaissance.⁴⁰ Hormis la preuve de concept d'Accenture mentionnée plus haut, d'autres projets visant à numériser les connaissances incluent, par exemple, une initiative de l'International Port Community Systems Association (IPCSA). En outre, en novembre 2017, la startup de technologie financière Wave a achevé avec succès un projet pilote mené avec ZIM, une société de transport israélienne, et avec Sparx Logistics de Hong Kong, Chine, en vue de délivrer et de transférer des connaissances électroniques en utilisant la technologie de la chaîne de blocs (Logistics and Fintech News, 2017).

La nécessité de numériser les diverses opérations le long de la chaîne de transport signifie que le développement de plates-formes commerciales mondiales nécessite des travaux d'intégration complexes et chronophages. Maersk et IBM reconnaissent que la plate-forme commerciale mondiale qu'ils ont élaboré ne s'étendra que progressivement, une ligne commerciale à la fois.

Les multiples projets en cours soulèvent également la question de l'interopérabilité. Les diverses plates-formes en cours d'élaboration vont-elles établir des normes différentes, au risque de créer un écheveau de normes ? En l'absence de normes garantissant que les plates-formes communiquent entre elles au niveau technique, mais également au niveau sémantique (types de renseignements devant être introduits et selon quel format), les efforts visant à numériser le commerce international ne resteront pas seulement limités, ils peuvent aussi recréer, à un autre niveau, les cloisons que la chaîne de blocs vise à supprimer (voir la section 4.2 b)). La coopération entre les différents acteurs d'un secteur, mais également entre les secteurs et avec les organisations de normalisation est primordiale pour éviter de dresser à nouveau des cloisons et des obstacles. Au niveau sectoriel, des initiatives voient le jour dans le secteur du transport routier, avec la création de la Blockchain in Transport Alliance (BiTA)⁴¹, un consortium de fabricants, de sociétés de transport terrestre et d'entreprises de logistique qui vise à élaborer des normes communes autour des applications de la chaîne de blocs dans le secteur du transport, de l'accélération des transactions à la sécurisation des transferts de données. Les membres de la BiTA représentent environ 85% de toutes les transactions liées au transport routier aux États-Unis et incluent des sociétés telles que UPS, SAP, US Xpress et Bridgestone, pour n'en citer que quelques-unes.

La chaîne de blocs s'annonce prometteuse en termes de numérisation du commerce international et de transformation du secteur du transport et de la logistique, mais elle ne peut réussir que si les sociétés travaillent main dans la main aux niveaux sectoriel et intersectoriel afin de définir les paramètres d'utilisation de la chaîne de blocs, ce qui demande un changement de paradigme culturel, à savoir de passer de

la concurrence à la collaboration – ou à la « concurrence coopérative ». Un dialogue ouvert entre toutes les parties prenantes participant au commerce international au sujet des normes est essentiel.

Enfin, l'intégration des services des douanes dans ces plates-formes soulève plusieurs questions réglementaires. Au-delà des difficultés liées aux processus G2G transfrontières (voir plus haut), le traitement des déclarations en douane sur la base des renseignements extraits d'une plate-forme commerciale mondiale basée sur la chaîne de blocs pourrait soulever des questions en termes de responsabilité. Les renseignements requis pour le dédouanement doivent généralement être présentés par un seul déclarant, qui en assume la responsabilité. Dans un système de chaînes de blocs, les renseignements peuvent être ajoutés par différentes parties prenantes, ce qui fait qu'il est impossible d'identifier un déclarant unique – à moins que le cadre réglementaire ne soit adapté pour clarifier les questions de responsabilité.

Comme les diverses initiatives en cours dans les domaines du financement du commerce, des procédures douanières, du transport et de la logistique le montrent, la chaîne de blocs ouvre de nouvelles possibilités de se rapprocher d'un commerce sans papier, mais différents défis techniques, réglementaires et de normalisation doivent être surmontés avant que la chaîne de blocs ne puisse véritablement réformer la façon dont les marchandises sont échangées au niveau international. Toutefois, compte tenu de l'impact potentiellement considérable que l'utilisation de la chaîne de blocs pourrait avoir sur les activités commerciales transfrontières, le temps et les efforts investis peuvent en valoir la peine. Si les défis techniques sont surmontés et que les essais en cours sont concluants, le commerce mondial pourrait, avec de la volonté politique, être radicalement différent dans 10 à 15 ans.

2. Une nouvelle génération de services ?

Les services sont un élément clé de l'activité économique et représentent plus de 60% de la production et de l'emploi dans le monde. Ces 20 dernières années, le commerce des services est devenu le segment le plus dynamique du commerce mondial; il augmente plus rapidement que le commerce des marchandises (OMC, 2015b). Le secteur des services, comme d'autres secteurs, a été affecté par l'essor des nouvelles technologies, en particulier Internet. De nouveaux modèles économiques ont émergé. L'apparition de la technologie de la chaîne de blocs pourrait encore changer la donne.

Dans quasiment tous les secteurs des services, un nombre croissant d'applications sont mises au point afin d'exploiter la technologie en vue de fournir de meilleurs services, plus rapidement et meilleur marché, sur une base nationale et

transnationale, ce qui met à rude épreuve les fournisseurs historiques bien établis. Hormis le financement du commerce, le transport et la logistique, qui ont été examinés dans la section précédente en raison du rôle clé qu'ils jouent dans le commerce international des marchandises, les autres services qui présentent un intérêt particulier pour le commerce international sont notamment les paiements transfrontières, les services d'assurance et la distribution.⁴²

(a) Services financiers

La chaîne de blocs trouve ses origines dans le secteur de la finance et, pour beaucoup, ce secteur est l'un de ceux dans lesquels l'utilisation de la technologie est la plus convaincante. Initialement mise au point dans le sillage de la crise financière mondiale de 2008 en guise d'alternative aux transactions financières centralisées, la chaîne de blocs est la technologie sur laquelle repose la désormais célèbre cryptomonnaie, bitcoin.

Toutefois, les chaînes de blocs sont beaucoup plus que des cryptomonnaies. Leurs applications potentielles vont bien au-delà du monde nébuleux des monnaies numériques, y compris dans le secteur de la finance. Un nombre croissant de banques, de sociétés financières, de bourses⁴³ et de startups étudient de quelle manière la technologie de la chaîne de blocs peut les aider à améliorer leurs activités. En fait, les banques comptent parmi les plus grands titulaires de brevets portant sur la technologie de la chaîne de blocs (20% de la totalité des brevets), derrière les sociétés spécialisées dans la chaîne de blocs mais devant les sociétés de technologie traditionnelles telles qu'IBM (Decker et Surrane, 2018). D'après McKinsey & Company, le secteur bancaire mondial devrait dépenser 400 millions de dollars EU dans des projets liés à la chaîne de blocs d'ici à 2019 (McKinsey & Company, 2017). Les démonstrations de faisabilité et les projets pilotes se multiplient, 70% environ des organismes financiers expérimentant déjà la technologie, tandis que de nouveaux modèles économiques susceptibles de transformer profondément le secteur de la finance voient le jour.

L'un des domaines dans lesquels la chaîne de blocs pourrait avoir un impact considérable est celui des paiements transfrontières, qui représentent environ 40% des recettes générées par les transactions de paiement à l'échelle mondiale (McKinsey & Company, 2016b). Les processus de paiement transfrontières ont déjà connu des modifications importantes au cours des dernières décennies avec l'émergence de nouveaux acteurs qui offrent aux clients et aux entreprises des solutions différentes, à valeur ajoutée, pour procéder aux paiements transfrontières par Internet ou via des téléphones mobiles. Les solutions de paiement électronique telles que PayPal, Amazon Payments et AliPay sont désormais largement utilisées. Dans les pays en développement, en particulier en Afrique, le faible niveau de

pénétration bancaire a conduit les fournisseurs de services mobiles à élaborer des solutions bancaires mobiles à titre d'alternative et de complément à la banque traditionnelle. L'utilisation de la banque mobile, c'est-à-dire du téléphone mobile, pour émettre et recevoir des paiements et réaliser d'autres opérations bancaires, s'est rapidement diffusée ces dernières années et prend une dimension transfrontières (OMC, 2016c). M-Pesa, qui a été lancé au Kenya en 2007 par Safaricom, le principal fournisseur de services mobiles du pays, est désormais utilisé par 70% de la population kenyane et s'est étendu à dix pays (Adegoke, 2017).

Un nombre croissant d'entreprises se tournent désormais vers la chaîne de blocs pour améliorer encore les paiements transfrontières. Un éventail d'acteurs non bancaires élaborent de nouveaux modèles économiques pour rendre les paiements transfrontières plus rapides et meilleur marché, ce qui conduit les établissements bien établis à s'adapter.

(i) La croissance de l'offre non bancaire

L'offre non bancaire est diversifiée et divisée en trois grandes catégories.

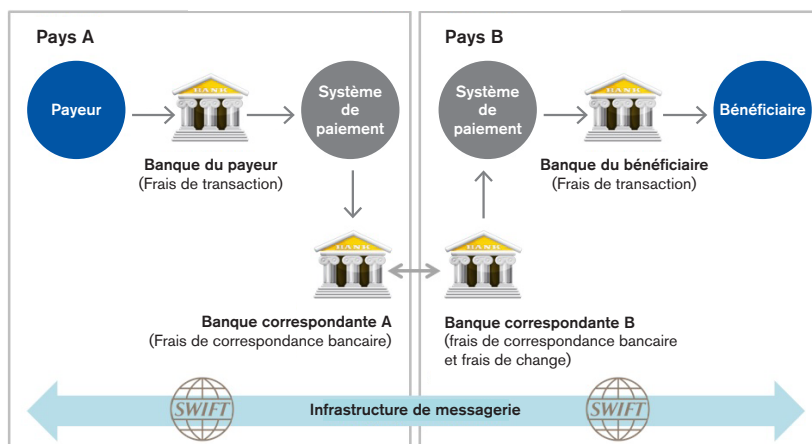
La première catégorie inclut les sociétés qui offrent la possibilité de traiter les paiements en cryptomonnaie, telles qu'AliPay, qui a récemment intégré une option bitcoin pour ses clients. De nombreuses startups, dont un grand nombre sont basées dans des pays en développement, proposent des paiements mondiaux basés sur des cryptomonnaies, tels que BitPesa au Kenya; BTCGhana; Bitso au Mexique; BitSpark à Hong Kong, Chine; OkCoin en Chine; OkLink/Coinsense en Inde; Rebit.ph et Coins.ph aux Philippines; Remitug en Ouganda; ainsi qu'Abra et Ripple aux États-Unis, etc. La liste est longue. Le nombre exponentiel de startups qui proposent des paiements transfrontières basés sur les cryptomonnaies dans les pays en développement semble suggérer que l'utilisation de la technologie de la chaîne de blocs et des cryptomonnaies pourrait avoir un fort impact sur les marchés qui sont mal desservis par les établissements financiers traditionnels. Nombreux sont ceux qui voient dans la chaîne de blocs un outil pour promouvoir davantage l'inclusion financière – pour « bancariser les exclus du système bancaire » – et une possibilité, pour les pays en développement, de faire l'impasse sur les technologies traditionnelles (voir, par exemple, International Finance Corporation (IFC) (2017)). Les partisans de la chaîne de blocs et des cryptomonnaies notent que cette technologie permet aux clients d'établir facilement une identité numérique, ce qui simplifie l'accès des populations non bancarisées aux services financiers, et qu'elle peut réduire encore davantage le coût des paiements transfrontières. Toutefois, le point de savoir si l'utilisation des cryptomonnaies permet effectivement de réduire encore le coût des paiements par rapport à la banque mobile dépend de la cryptomonnaie utilisée, puisque les frais de transaction moyens peuvent varier de

zéro à plus de 7 dollars EU (Ohnesorge, 2018), sans même prendre en considération l'extrême volatilité de la plupart des cryptomonnaies. En outre, les paiements transfrontières en cryptomonnaie présentent l'inconvénient de nécessiter une connexion Internet, alors que certains systèmes de paiement mobile demandent seulement un téléphone mobile ordinaire, ce qui est un élément important dans les pays en développement. Par conséquent, le point de savoir si l'utilisation des cryptomonnaies pour les paiements transfrontières fera réellement diminuer les coûts, favorisera l'inclusion financière et bouleversera encore davantage le secteur est une question qui reste ouverte.

La deuxième catégorie comprend les sociétés qui exploitent la technologie de la chaîne de blocs pour offrir aux utilisateurs finals des solutions de paiement transfrontières en monnaies fiduciaires* rapides, sûres et bon marché via des réseaux de pair à pair. La startup Circle, par exemple, propose des paiements transfrontières basés sur la chaîne de blocs en monnaies fiduciaires sans frais ni majoration de change. La société, qui a commencé ses activités aux États-Unis avant de déménager en Europe, est récemment entrée sur le marché chinois dans l'objectif de relier les consommateurs chinois au reste du monde (Lomas, 2016). Traxpay⁴⁴, de son côté, a créé une plate-forme basée sur la chaîne de blocs qui permet aux entreprises d'une chaîne d'approvisionnement d'effectuer entre elles des paiements en temps réel, en contournant les banques et les instruments traditionnels de financement du commerce – une sorte de PayPal pour le monde B2B. Reste à savoir si ces sociétés réussiront à s'établir comme des acteurs majeurs sur le marché.

La troisième catégorie inclut les sociétés qui exploitent la technologie de la chaîne de blocs pour remettre en cause le manque d'efficacité du système de correspondance bancaire actuel. En effet, les banques continuent d'utiliser une infrastructure complexe pour transférer de l'argent à l'étranger, les paiements transfrontières étant souvent acheminés via une série de contreparties. Lorsque des paiements transfrontières doivent être effectués entre des banques qui ne disposent pas d'un accord établi, une banque correspondante doit être utilisée comme intermédiaire (voir la figure 11). Étant donné que de nombreuses banques dans le monde n'ont pas d'arrangements bancaires établis les unes avec les autres, la banque du payeur choisit souvent d'utiliser le réseau SWIFT pour rechercher une banque correspondante ayant conclu des accords avec la banque du bénéficiaire ou une autre banque correspondante sur le territoire de la banque du bénéficiaire. La banque du payeur envoie alors les fonds transférés sur le compte qu'elle détient auprès de la banque correspondante, qui prélève des frais et envoie l'argent à la banque correspondante étrangère ou à la banque réceptrice.

La correspondance bancaire demande généralement que les deux banques établissent entre elles des comptes réciproques, habituellement appelés comptes

Figure 11 Modèle de correspondance bancaire

Source: Barry et Zaccardi (2015).

«vostro» ou «nostro».⁴⁵ Ces comptes correspondants permettent aux banques de gérer les paiements transfrontières nécessitant des opérations de change, tels que ceux qui sont effectués lorsque des marchandises sont importées en provenance d'un pays étranger.

La participation de multiples établissements financiers augmente les coûts et les délais. Les banques correspondantes facturent généralement leurs services entre 20 et 60 dollars EU en plus de l'écart de change en vigueur et, alors que la plupart des paiements transfrontières pourraient en théorie être exécutés en un ou deux jours, une étude menée par McKinsey en 2015 a révélé qu'il faut compter entre trois et cinq jours ouvrables pour effectuer un paiement de détail transfrontières ordinaire (McKinsey & Company, 2016c).

Le manque d'efficacité du système actuel a conduit des startups, telles que Ripple, à mettre au point d'autres solutions basées sur la chaîne de blocs.⁴⁶ Ripple essaie de transformer les systèmes de paiement – qui sont souvent considérés comme lents, d'une transparence limitée et onéreux – grâce à sa plate-forme d'échange de valeurs basée sur la chaîne de blocs. La plate-forme Ripple permet aux établissements financiers d'échanger, en temps réel et à moindre coût, voire gratuitement, des monnaies, des cryptomonnaies, des produits de base et autres jetons de valeur directement, sans s'appuyer sur les intermédiaires traditionnels du système financier international. Le processus est bilatéral et instantané. Lorsqu'un ordre de paiement est introduit sur la plate-forme, les fournisseurs de liquidités reliés à la plate-forme entrent en concurrence pour proposer le meilleur taux de change. Ripple choisit alors automatiquement le meilleur taux pour effectuer le

paiement. D'après Ripple, l'ensemble du processus prend entre trois et six secondes.⁴⁷

Ripple a des licences avec plus de 100 banques et établissements financiers et a pour ambition de transformer les paiements transfrontières en une activité véritablement mondiale. La possibilité de contourner les banques correspondantes pourrait s'avérer particulièrement intéressante pour les pays en développement, qui ont été confrontés à un déclin du nombre de relations de correspondance bancaire actives à la suite de la crise financière de 2018 compte tenu de l'augmentation des coûts de mise en conformité découlant dans une large mesure de prescriptions réglementaires plus strictes en matière de connaissance du client et de lutte contre le blanchiment d'argent. Les coûts du maintien d'une relation de correspondance de base sont passés de 15 000 euros à 75 000 euros par relation (Chambre de commerce internationale (ICC), 2017a), montant qui, pour de nombreuses banques de pays en développement, est intenable compte tenu du volume réel des transactions à gérer dans le cadre de ces relations. Les régions ayant le nombre le plus faible de relations de correspondance bancaire actives sont l'Amérique latine, l'Océanie et l'Afrique (Financial Stability Board (FSB), 2018).

Toutefois, pour l'instant, malgré le nombre élevé de banques qui ont adhéré au réseau, il semble que seul un nombre limité de grandes opérations aient effectivement été réalisées. Les banques testent encore le système (Leising et Robinson, 2018).

D'autres grandes sociétés, telles qu'IBM avec sa plate-forme Blockchain World Wire et Ant Financial, société affiliée d'Alibaba, travaillent également sur des produits similaires.

Une autre initiative digne d'intérêt est le service de paiements transfrontières basé sur la chaîne de blocs lancé en octobre 2017 par IBM, KlickEx Group – société de services financiers du Pacifique financée par l'ONU – et Stellar.org, une organisation à but non lucratif qui supporte un réseau de chaîne de blocs libre pour les services financiers. Le service vise à améliorer l'efficacité et à réduire le coût des paiements transfrontières dans la région du Pacifique en permettant l'échange électronique de 12 monnaies différentes entre l'Australie, la Nouvelle-Zélande, les îles du Pacifique et le Royaume-Uni. Le service, qui traite déjà des transactions en direct dans la région du Pacifique, devrait s'étendre à d'autres régions du monde (Mearian, 2017).

Il est encore trop tôt pour dire si ces initiatives se développeront à l'échelle mondiale et si elles modifieront profondément la façon dont les paiements transfrontières sont effectués. Pour offrir des alternatives valables au système existant de correspondance bancaire, les applications de la chaîne de blocs pour les paiements

transfrontières devraient relier toutes les monnaies et tous les établissements financiers du monde – «une entreprise massive» comme le notent McKinsey & Company dans une étude de 2016 (McKinsey & Company, 2016c), voire une utopie. En outre, la construction d'un réseau mondial pour les paiements transfrontières peut être difficile sur le plan technique, voire impossible compte tenu de l'état actuel de la technologie, à moins de sacrifier la rapidité et l'efficacité. Toutefois, il est clair que l'émergence de nouveaux modèles économiques qui court-circuitent les intermédiaires traditionnels a bouleversé le monde de la finance, ce qui conduit les établissements financiers à s'adapter.

(ii) Initiatives des établissements financiers

Un éventail d'établissements financiers bien établis examinent actuellement le potentiel de la chaîne de blocs (voir la figure 12).

En janvier 2017, SWIFT a lancé une application de preuve de concept afin de déterminer si la chaîne de blocs pourrait être utilisée pour améliorer le rapprochement bancaire des comptes nostro en temps réel, en réduisant les coûts et les risques opérationnels et en optimisant la liquidité globale des banques. En effet, dans le système actuel, les banques doivent suivre les fonds disponibles sur leurs comptes à l'étranger via des mises à jour de débit et de crédit et des relevés de compte de fin de journée. La gestion et la notification des paiements interbancaires représentent une part importante du coût des paiements transfrontières. D'après SWIFT, en moyenne 34% des coûts d'une transaction internationale sont liés à des liquidités bloquées dans un compte nostro du fait de l'absence de données en temps réel, et 9% sont imputables à des enquêtes et exceptions principalement dues à un manque de standardisation du processus de paiement de bout en bout et au rapprochement avec le compte nostro connexe. Les banques ont mentionné le rapprochement avec le compte nostro comme un point particulièrement difficile (SWIFT, 2018a).

D'après le rapport final de SWIFT sur la preuve de concept concernant les comptes nostro publié en mars 2018, la chaîne de blocs a rempli les fonctionnalités opérationnelles escomptées, y compris la gestion en temps réel, la mise à jour du statut des transactions, la fourniture de pistes d'audit complètes, la visibilité des soldes escomptés et disponibles et la confirmation en temps réel des écritures comptables simplifiées. Toutefois, la valeur de la solution basée sur la chaîne de blocs dépend des capacités de gestion des liquidités, ainsi que du niveau d'automatisation et de centralisation de la banque. Alors que les grandes banques disposent généralement de leurs propres structures internes pour gérer l'information sur les liquidités – dont un grand nombre fonctionnant en temps réel – et ne voient peut-être pas la nécessité d'intégrer une solution basée sur la chaîne de blocs dans leurs systèmes et processus existants, une solution de ce type pourrait être très

Divers consortiums se sont formés, le plus connu étant R3 (R3CEV LLC), qui a débuté ses activités en 2015 avec neuf sociétés financières : Barclays, BBVA, la Commonwealth Bank of Australia, Crédit Suisse, Goldman Sachs, J.P. Morgan, la Royal Bank of Scotland, State Street et UBS. R3 compte désormais plus de 200 banques, sociétés d'assurance, établissements financiers, organismes de réglementation, associations commerciales et sociétés de technologie parmi ses membres. Le consortium, qui a créé une technologie de registre distribué en code source ouvert appelée Corda «entièrement conçue pour enregistrer, gérer et synchroniser les accords financiers entre établissements financiers réglementés» (Brown, 2016), a annoncé en octobre 2017 le lancement d'une plate-forme de paiements transfrontières basée sur la technologie Corda (Brady, 2017). La plate-forme a pour objectif de favoriser une exécution plus rapide et plus efficace des opérations de paiements transfrontières.

En outre, plusieurs établissements financiers bien établis ont récemment annoncé le lancement de leurs propres réseaux de chaînes de blocs pour améliorer les processus de paiement transfrontières.

En octobre 2017, Mastercard a lancé son propre réseau de chaînes de blocs pour faire face aux problèmes de rapidité, de transparence et de coûts des paiements transfrontières entre entreprises (B2B). La chaîne de blocs de Mastercard est un registre avec permission accessible via une API, ce qui permet aux utilisateurs de se connecter à la chaîne de blocs sans avoir à créer leurs propres nœuds* serveurs de registre distribué (Mastercard, 2017).

En novembre 2017, Visa a lancé la première phase pilote de son service de paiement B2B basé sur la chaîne de blocs, B2B Connect, annoncé pour la première fois l'année précédente (De, 2017). La plate-forme vise à faciliter les paiements transfrontières en favorisant les paiements directs entre établissements, en supprimant les intermédiaires traditionnels. La Commerce Bank, basée aux États-Unis, la Shinhan Bank de la République de Corée, l'UnionBank des Philippines et l'United Overseas Bank, basée à Singapour, collaborent avec Visa sur ce projet.

Le même mois, J.P. Morgan a lancé le réseau Interbank Information Network (IIN), basé sur la chaîne de blocs, en collaboration avec la Royal Bank of Canada et l'Australia and New Zealand Banking Group Limited. IIN exploite la technologie de la chaîne de blocs pour «réduire au minimum les frictions dans les processus de paiements internationaux» en permettant des paiements plus rapides, nécessitant moins d'étapes, et réalisés de façon plus sûre (J.P. Morgan, 2017).

Avec ses promesses d'efficacité accrue, de règlements plus rapides à un coût moindre, de risque de fraude réduit, de traçabilité vérifiable et de pressions

croissantes de la part des innovateurs numériques, la chaîne de blocs est considérée par de nombreux établissements financiers comme une technologie «digne d'être étudiée». Les économies générées par l'utilisation de cette technologie pourraient potentiellement être importantes. D'après Santander *et al.*, (2015), la chaîne de blocs pourrait réduire les coûts d'infrastructure des banques attribuables aux paiements transfrontières, au négoce des valeurs mobilières et au respect de la réglementation de 15 à 20 milliards de dollars EU par an d'ici à 2022.

La chaîne de blocs sera-t-elle l'avenir des paiements transfrontières ? Le temps le dira. La technologie continue à évoluer et son potentiel est encore à l'étude. Les incertitudes réglementaires et le manque d'interopérabilité des plates-formes actuelles représentent toujours un défi (voir la section 4.2). Par conséquent, tout porte à croire que l'adoption se fera progressivement. Il est probable que les établissements financiers bien établis se concentreront d'abord sur les activités internes afin d'améliorer l'efficacité et de réduire la complexité organisationnelle et les coûts de back-office – notamment parce que, à l'heure actuelle, certaines grandes banques réalisent des profits considérables sur les transactions transfrontières et pourraient ne pas être enclines à adopter une technologie qui pourrait les priver de l'une de leurs principales sources de revenus.

Toutefois, une chose est sûre : la chaîne de blocs bouleverse le secteur et pousse des établissements financiers bien établis à s'adapter. Si les applications développées récemment sont concluantes et que les questions d'interopérabilité sont résolues, ce qui permettrait de relier différentes plates-formes de paiement, la chaîne de blocs pourrait bien devenir l'avenir de l'infrastructure des services financiers ; cependant, il est peu probable que l'on assiste à un remodelage et à une décentralisation complets de l'environnement financier. Ironiquement, ce sont ceux que Satoshi Nakamoto, le «père» de la technologie de la chaîne de blocs, voulait rendre superflus qui plaident désormais la cause de cette technologie en tant que moyen d'améliorer leur propre fonctionnement. En définitive, la chaîne de blocs pourrait bien contribuer à renforcer ces établissements financiers bien établis.

(b) Assurance

Le monde des services financiers n'est pas le seul secteur des services à connaître des bouleversements liés à cette technologie. La chaîne de blocs commence également à exercer une influence dans le secteur de l'assurance. Toutes les grandes sociétés de conseil, y compris McKinsey & Company, Ernst & Young, Deloitte, PricewaterhouseCoopers et KMPG, ont récemment publié des études sur le potentiel de la chaîne de blocs dans ce secteur⁴⁸, et des sociétés d'assurance telles qu'Axa, Generali, Allianz, Aegon, Munich Re, Swiss Re et Zurich, pour n'en citer que quelques-unes, investissent dans cette technologie.

Le potentiel de la chaîne de blocs dans le secteur de l'assurance est multiforme. L'utilisation de la chaîne de blocs et des contrats intelligents pourrait aider à réduire les procédures et les coûts administratifs grâce à la vérification automatisée de l'identité du titulaire d'une police et de la validité d'un contrat et à la gestion automatisée des déclarations de sinistres. Lorsqu'une déclaration de sinistre est présentée, le réseau pourrait aider à s'assurer qu'elle est valable et que des déclarations multiples n'ont pas été envoyées pour le même incident, ce qui réduirait la fraude – celle-ci étant estimée à 5 à 10% de l'ensemble des déclarations (McKinsey & Company, 2016a). Des contrats intelligents pourraient permettre de déclencher automatiquement les paiements lorsque certaines conditions qui y sont spécifiées sont réunies. La chaîne de blocs pourrait simplifier les procédures administratives, renforcer la confiance et la transparence, accélérer la liquidation des sinistres et aider le secteur de l'assurance à gérer les transactions d'une façon qui est non seulement plus sûre mais aussi plus responsable envers ses clients.

L'application de la chaîne de blocs fait également l'objet d'essais dans le domaine des polices d'assurance multinationales. En juin 2017, AIG, IBM et Standard Chartered Bank ont annoncé qu'elles avaient mené avec succès un projet pilote portant sur la première police d'assurance multinationale basée sur un contrat intelligent utilisant la chaîne de blocs (IBM, 2017). La police mère au Royaume-Uni et trois polices locales au Kenya, à Singapour et aux États-Unis, ont été converties en un contrat intelligent qui permet de disposer d'une vision partagée des données et des documents relatifs aux polices en temps réel et d'automatiser les procédures, d'accroître la transparence, la confiance et l'efficacité de la gestion du processus. Les sociétés ont annoncé que l'utilisation de la chaîne de blocs permettait une visibilité totale de la couverture et du paiement de la prime au niveau local et au niveau principal, ainsi que des notifications automatisées aux participants du réseau à la suite de transferts des paiements, et que le processus d'élaboration de la police multinationale, qui pouvait demander des mois, était réduit à quelques jours.

Un aspect particulièrement intéressant pour le commerce international est l'impact potentiel que la technologie peut avoir sur le secteur de l'assurance maritime. Puisque 90% des échanges internationaux sont effectués par voie maritime, l'assurance maritime joue un rôle crucial dans le commerce international. Pour faire face à la diversité des risques auxquels le fret est exposé – des dommages causés aux marchandises aux retards dus à l'engorgement des ports – les expéditeurs contractent des assurances auprès de multiples courtiers et assureurs. Ce secteur, qui représente 30 milliards de dollars EU, repose encore beaucoup sur le papier et, jusqu'à présent, peu d'efforts avaient été déployés pour optimiser les coûts et les processus. Un projet récent concernant l'assurance maritime mise au point par Maersk, Microsoft, Ernst & Young et plusieurs sociétés d'assurance pourrait changer la donne. Leur plate-forme de chaîne de blocs Insurwave, fondée sur la technologie

d'informatique en nuage Azure de Microsoft, permet à toutes les parties – y compris les sociétés de transport, les courtiers, les assureurs et autres fournisseurs – d'accéder au même registre, qui est mis à jour en temps réel et peut être utilisé pour des contrats d'assurance maritime (Kelly, 2017). La plate-forme vise à accélérer les processus de facturation et de paiement et à assurer une plus grande transparence, en particulier en ce qui concerne les antécédents de sinistres, afin de mieux éclairer les décisions en matière de fixation des prix, tout en garantissant une plus grande sécurité des données et des transactions. Le consortium a commencé à tester le système en avril 2017 et a mis au point une douzaine de cas d'utilisation. L'exploitation commerciale du nouveau système d'assurance maritime a commencé en janvier 2018. Le système sera d'abord utilisé pour un nombre limité de navires et de trajets avant d'être déployé plus largement, éventuellement pour d'autres catégories d'assurance telles que l'assurance automobile (Ralph, 2017).

Comme dans le cas des services financiers, l'utilisation de la chaîne de blocs pourrait profondément transformer le secteur de l'assurance, y compris dans sa dimension multinationale. Les applications passent désormais des démonstrations de faisabilité à la mise en œuvre. Les années à venir nous diront si la chaîne de blocs change réellement les règles du jeu.

(c) Distribution de détail/commerce électronique⁴⁹

La distribution de détail a connu une transformation radicale au cours des 10 ou 20 dernières années. L'essor d'Internet a profondément modifié les comportements des consommateurs, un nombre croissant d'entre eux effectuant des achats en ligne. La société d'études de marché eMarketer estime que les ventes de détail en ligne ont augmenté de 23% en 2017 pour atteindre presque 2 300 milliards de dollars EU. Environ 10% des ventes de détail sont réalisées en ligne, chiffre qui devrait dépasser 16% d'ici à 2021 les ventes totales en ligne atteignant presque 4 500 milliards de dollars EU (eMarketer, 2017). La numérisation de la distribution de détail a également donné naissance à de nouveaux modèles économiques et à l'émergence de grandes plates-formes de commerce électronique telles qu'Amazon et Alibaba.

L'utilisation de la chaîne de blocs pour les ventes en ligne pourrait avoir une influence sur le paysage actuel du commerce électronique à plusieurs égards.

D'abord, la chaîne de blocs pourrait offrir aux clients des solutions plus sûres et plus rapides, ce qui pourrait contribuer à accroître le nombre de clients et à stimuler les ventes en ligne. Les plates-formes traditionnelles de commerce électronique manquent souvent de transparence. Un système de commerce électronique basé sur la chaîne de blocs permet de suivre facilement les registres des transactions

précédentes, et des contrats intelligents peuvent faciliter les transactions en permettant des transferts de paiement automatiques. Le caractère immuable de la chaîne de blocs peut également aider à prévenir la fraude en facilitant le suivi des marchandises contrefaites et des comportements frauduleux. Le caractère transparent de la chaîne de blocs et la possibilité qu'offre cette technologie de lutter contre la fraude et les marchandises contrefaites sont les aspects qui ont poussé le géant du commerce en ligne Alibaba à investir massivement dans la chaîne de blocs (voir la section 4.1 a)).

Ensuite, la chaîne de blocs peut être utilisée pour mettre en œuvre un marché de pair à pair qui fonctionne sans qu'un acteur central ne soit nécessaire. De nouveaux acteurs utilisant la chaîne de blocs pour offrir aux clients un accès direct aux vendeurs sans qu'ils aient besoin de passer par une plate-forme centralisée telle qu'Amazon voient le jour. OpenBazaar, par exemple, est un marché de pair à pair en ligne gratuit lancé en novembre 2017, sur lequel il est possible de vendre et d'acheter des marchandises sans avoir à créer de compte. Il n'y a pas de frais d'inscription ni de frais de plate-forme. Un contrat intelligent bloque les fonds une fois que le paiement a été effectué et les libère lorsque l'acheteur reçoit et vérifie l'article.⁵⁰ Pour l'instant, la portée de ces initiatives reste très limitée. Le point de savoir si ces plates-formes offriront des avantages réels par rapport aux plates-formes existantes et parviendront à devenir des acteurs clés reste à déterminer.

La chaîne de blocs commence tout juste à entrer dans l'univers du commerce électronique. Elle ne va peut-être pas le révolutionner, mais en renforçant la sécurité, la confiance et la transparence, et éventuellement en facilitant les paiements, y compris les paiements transfrontières (voir la section 3.2 a)), elle pourrait donner au commerce électronique un nouvel élan et affecter les modèles économiques existants.

La chaîne de blocs est en train de rapidement pénétrer le monde des services. Tant les entreprises bien établies que les startups se tournent vers celle-ci pour fournir des services améliorés dans des domaines aussi divers que le financement de la chaîne d'approvisionnement, les paiements transfrontières, l'assurance, le transport et la logistique, et même le commerce électronique. Un bouleversement important des relations de pouvoir dans un secteur est toutefois peu probable. Si « révolution » il y a, elle sera plus probablement interne : les caractéristiques intrinsèques de la chaîne de blocs et la possibilité d'automatiser les transactions grâce aux contrats intelligents en font un outil attrayant pour les entreprises qui leur permet de réduire les coûts et de simplifier les processus. Si les initiatives en cours s'avèrent concluantes, la chaîne de blocs pourrait bien devenir la future « infrastructure » du secteur des services. En raison de ses capacités d'automatisation, la chaîne de

blocs pourrait être au secteur des services ce que les robots ont été à l'industrie manufacturière.

3. Renforcement des droits de propriété intellectuelle

La propriété intellectuelle est un aspect de plus en plus important du commerce international. De nombreux produits, des nouveaux médicaments et produits pharmaceutiques aux produits de haute technologie tels que les smartphones, demandent des investissements importants dans la recherche et la conception. En fait, la majeure partie de la valeur de ces produits dépend de la quantité d'innovation, d'idées et de connaissances mise en jeu. Les enregistrements musicaux, les films, les livres, les logiciels informatiques sont des produits créatifs qui sont achetés et vendus pour les idées qu'ils contiennent plutôt que pour le support ou le médium utilisé pour les échanger.

La protection de la propriété intellectuelle est devenue une préoccupation essentielle des entreprises, des créateurs et des innovateurs. Ces dernières décennies, un ensemble complet de règles a été élaboré aux niveaux national et multilatéral afin de fournir une protection adéquate de la propriété intellectuelle et de garantir une rémunération équitable des créateurs et des innovateurs. L'Accord de l'OMC sur les aspects des droits de propriété intellectuelle qui touchent au commerce (Accord sur les ADPIC), qui est entré en vigueur le 1^{er} janvier 1995, fournit un cadre général de normes minimales pour la protection et le respect des droits de propriété intellectuelle applicable à tous les Membres de l'OMC. Il inclut des disciplines sur le droit d'auteur et les droits connexes (c'est-à-dire les droits des artistes interprètes ou exécutants, des producteurs d'enregistrements sonores et organismes de radiodiffusion); les marques de fabrique ou de commerce; les indications géographiques; les modèles et dessins industriels; les brevets; les schémas de configuration de circuits intégrés; et les renseignements non divulgués, y compris les secrets commerciaux et les données résultant d'essais. L'Organisation mondiale de la propriété intellectuelle (OMPI) administre pas moins de 26 traités qui visent l'ensemble des droits de propriété intellectuelle (DPI). Les principaux traités de l'OMPI relatifs aux droits d'auteur, aux brevets, aux marques de fabrique et de commerce et aux dessins et modèles industriels sont intégrés par référence dans l'Accord sur les ADPIC. Un nombre croissant d'accords de libre-échange contiennent également des dispositions relatives à la propriété intellectuelle.

Les règles existent, mais l'administration et le respect restent, dans de nombreux cas, un défi. Le droit d'auteur ne nécessitant pas d'enregistrement et étant disponible dès la création de l'œuvre originale, il peut être difficile, et parfois impossible, de déterminer le détenteur du droit. En conséquence, les auteurs et les artistes

interprètes ou exécutants se battent souvent pour être rémunérés pour leur création et, lorsqu'ils y parviennent, une grande part de leurs recettes est souvent accaparée par des intermédiaires tels que des labels ou des maisons de disque, des organismes de gestion des droits d'exécution et des fournisseurs de services numériques en flux continu tels que Spotify, dans le cas de la musique. Cette situation a attiré l'attention des Membres de l'OMC. Le Brésil, dans une communication présentée au Conseil général de l'OMC en décembre 2016, a demandé une « décision... sur la gestion du droit d'auteur en vue d'une rémunération équitable des auteurs et des artistes interprètes et exécutants » dans laquelle les Membres de l'OMC « soulign[ai]ent l'importance... de [la] transparence dans la rémunération du droit d'auteur et des droits voisins dans l'environnement numérique » (OMC, 2016a).

Dans une communication complémentaire distribuée en septembre 2018, le Brésil et l'Argentine notent que « [l]es technologies de l'information pourraient et devraient faciliter l'accès à des données en temps réel sur l'utilisation et la rémunération des détenteurs de droits » (OMC, 2018).

Le piratage portant atteinte à un droit d'auteur et le commerce des produits de contrefaçon sont également particulièrement préoccupants. D'après l'OCDE et l'Office de l'Union européenne pour la propriété intellectuelle (EUIPO), la valeur des importations de marchandises contrefaites et pirates avoisine 500 milliards de dollars EU par an – environ 2,5% des importations mondiales –, les marques françaises, italiennes et américaines étant les plus durement touchées (OCDE-EUIPO, 2016) et, selon les estimations de l'OMS, 10 à 30% des médicaments en vente dans les pays en développement pourraient être contrefaits, causant 700 000 décès par an dans le monde (Organisation mondiale de la santé, 2016).

L'une des spécificités des droits de propriété intellectuelle (DPI) est qu'ils sont par nature territoriaux. Ils sont conférés, protégés et opposables séparément dans différentes juridictions dans le monde. Les droits accordés dans une juridiction ne sont protégés et opposables que dans cette juridiction. Par exemple, l'utilisation d'un brevet dans une juridiction autre que celle dans laquelle le brevet a été accordé ne serait pas nécessairement considérée comme une atteinte aux droits.

La chaîne de blocs peut-elle aider à répondre à ces défis en matière d'administration des droits, de moyens de les faire respecter et de territorialité ? L'utilisation de la chaîne de blocs dans le domaine de la propriété intellectuelle est encore relativement nouvelle, mais elle pourrait ouvrir des possibilités intéressantes. L'écosystème de sociétés qui examinent de quelle manière la technologie de la chaîne de blocs peut être utilisée pour améliorer l'administration des DPI et les moyens de les faire respecter dans de multiples juridictions s'étend rapidement. Les applications de la

chaîne de blocs sont nombreuses et pourraient affecter à la fois la gouvernance des DPI et le secteur de la propriété intellectuelle. S'agissant des droits enregistrés et non enregistrés, la chaîne de blocs pourrait sans doute être utilisée pour apporter la preuve de la création, de la titularité et de la première utilisation; pour enregistrer les DPI; pour administrer et gérer les DPI, y compris les paiements; et pour faire respecter les DPI et lutter contre les contrefaçons. Toutefois, même si les applications de la technologie de la chaîne de blocs peuvent contribuer à répondre à certains défis auxquels les détenteurs de droits sont confrontés, la technologie ne résoudra pas tous les problèmes.

(a) Preuve d'existence et titularité

Apporter la preuve de la titularité d'œuvres littéraires ou artistiques, de marques de fabrique ou de commerce, de brevets ou de modèles et dessins industriels est essentiel si l'on souhaite faire valoir une protection de la propriété intellectuelle. Cependant, comme cela a déjà été mentionné, la détermination de la titularité peut s'avérer difficile, en particulier dans le cas du droit d'auteur.

(i) *Droit d'auteur*

Les œuvres littéraires ou artistiques telles que les dessins, les peintures et les œuvres littéraires, musicales, cinématographiques et photographiques sont protégées dès lors qu'elles ont été «fixées sur un support matériel».⁵¹ Aucun enregistrement n'est nécessaire. Toutefois, dans les juridictions dans lesquelles les auteurs et les artistes interprètes ou exécutants n'ont pas les moyens adéquats de répertorier leurs œuvres, la titularité peut être difficile à prouver.

Il pourrait être particulièrement intéressant d'utiliser la chaîne de blocs pour prouver la titularité d'œuvres littéraires et artistiques numériques. La chaîne de blocs pourrait fournir aux auteurs et aux artistes interprètes ou exécutants de ces œuvres une preuve de titularité immuable, sûre et horodatée.* Les œuvres numériques créées directement sur des applications utilisant cette technologie pourraient être «enregistrées» instantanément, dès leur création.

Les avantages potentiels qu'offre l'utilisation de cette technologie pour enregistrer le droit d'auteur sont très variés: les entrées ajoutées à la chaîne de blocs ne peuvent pas être dupliquées, manipulées ni falsifiées; elles sont permanentes; et les renseignements stockés peuvent facilement être retracés, ce qui permet d'assurer plus facilement le respect des DPI. Certaines sociétés telles que Binded (anciennement Blockai), Ascribe, Blocknotary, Copyrobo et KodakOne offrent déjà aux auteurs et aux artistes interprètes ou exécutants la possibilité d'enregistrer leurs œuvres numériques sur des applications de la chaîne de blocs et les services

fournissant une preuve d'existence pour tout type d'œuvre, y compris le droit d'auteur, se sont multipliés ces dernières années.⁵² Binded⁵³, par exemple, aide les artistes à revendiquer leurs droits d'auteur et à les protéger en leur permettant de placer leur art numérique et leurs photos sur sa plate-forme de droit d'auteur. La société crée un horodatage dans la chaîne de blocs et délivre un certificat de droit d'auteur comme preuve d'authenticité. Bien que le nombre d'utilisateurs de ces sociétés reste encore limité pour le moment, celles-ci offrent une solution intéressante pour les artistes et les créateurs qui souhaitent apporter la preuve de la titularité de leurs œuvres numériques.

Toutefois, dans le cas des œuvres non numériques, la chaîne de blocs peut seulement apporter une preuve d'existence, pas de titularité. La chaîne de blocs ne peut pas garantir la fiabilité des renseignements saisis dans le registre. Elle peut seulement garantir que les renseignements inclus dans le registre n'ont pas été falsifiés. L'enregistrement dans la chaîne de blocs ne peut donc pas résoudre les questions liées à l'acquisition illégale d'œuvres créatives. L'enregistrement dans la chaîne de blocs ne peut pas garantir que la personne qui enregistre l'œuvre est le créateur originel de l'œuvre. Il prouve seulement que, au moment où les données ont été ajoutées au registre, l'œuvre existait – preuve d'existence – et était en possession de la personne qui l'a enregistrée. Un système de vérification physique sera toujours nécessaire. Dans le cas d'œuvres non numériques, les œuvres originales ne peuvent pas être stockées sur la chaîne de blocs; seul le condensé cryptographique* de l'œuvre peut l'être. Comme le hachage* crée une empreinte qui est propre à l'œuvre à laquelle il renvoie, il constitue certes une garantie d'authenticité, mais pas une garantie de titularité.

(ii) Marques de fabrique ou de commerce

S'agissant des marques de fabrique et de commerce, les droits de titularité sont obtenus par la partie qui utilise ou enregistre en premier un signe particulier (par exemple, un terme, un logo, une expression ou un dessin ou modèle) auprès d'une autorité centrale. Une preuve de première utilisation ou de premier enregistrement est donc essentielle.

Dans les juridictions dans lesquelles une preuve de première utilisation est exigée, la chaîne de blocs pourrait être utilisée pour créer une entrée cryptographique horodatée d'une marque de fabrique ou de commerce qui pourrait ensuite servir de preuve de première utilisation. Dans les juridictions exigeant un enregistrement, les autorités centrales chargées de l'enregistrement des marques de fabrique ou de commerce pourraient choisir de tirer profit du caractère immuable et transparent de la technologie de la chaîne de blocs pour améliorer l'enregistrement et la gestion des DPI.

Bien que certains offices de la propriété intellectuelle, tels que l'EUIPO, semblent envisager d'utiliser la chaîne de blocs pour enregistrer et faire respecter les DPI (Mertens, 2018b), les organismes gouvernementaux ne passeront pas du jour au lendemain à un système basé sur la chaîne de blocs. Dans l'intervalle, des startups passent à l'action, au risque de créer une confusion et d'éventuels conflits entre deux types d'enregistrement différents (Monteleone, 2018). Aux États-Unis, la startup Cognate⁵⁴, par exemple, utilise la chaîne de blocs pour délivrer des « marques de chaîne » – au lieu de marques de fabrique ou de commerce. Les sociétés peuvent télécharger une preuve d'utilisation de la marque de fabrique ou de commerce et d'autres renseignements sur leur marque. Après examen des documents, la société enregistre la marque en tant que « marque de chaîne ». Le processus est simple et rapide : il ne demande qu'un jour et coûte environ 40 dollars EU, tandis que l'enregistrement auprès d'organismes gouvernementaux tels que l'Office des brevets et des marques des États-Unis (USTPO) ou l'EUIPO peut prendre jusqu'à 12 mois, avec des frais beaucoup plus élevés (Mertens, 2018b).

Ces initiatives soulèvent la question du statut juridique de l'« enregistrement » des marques de fabrique ou de commerce via des plates-formes basées sur la chaîne de blocs avec permission en cas de litige. Cet enregistrement pourrait être utile pour apporter la preuve de la première utilisation, mais ces « marques de chaîne » seront-elles opposables auprès des tribunaux, comme le sont les marques de commerce et de fabrique ? Offriront-elles le même niveau de protection que les marques de fabrique ou de commerce traditionnelles ?⁵⁵ Les règles existantes devraient-elles être adaptées pour tenir compte de ces évolutions ? Ces questions méritent d'être examinées ; le caractère potentiellement disruptif de la technologie de la chaîne de blocs occupera probablement les juristes et les autorités de réglementation dans les années à venir.

(iii) Brevets

La chaîne de blocs pourrait aussi faciliter l'enregistrement des brevets. Un brevet est un droit juridique accordé par un office national ou régional des brevets pour une certaine durée – au moins 20 ans – à un inventeur qui a créé quelque chose de nouveau, qui implique une activité inventive et qui peut faire l'objet d'une application industrielle. Les demandes de brevet sont gérées au niveau national ou régional par quelque 200 offices des brevets, dont certains étudient déjà la capacité de la chaîne de blocs à les aider à simplifier leurs activités (Mertens, 2018a). Au-delà de l'utilisation institutionnelle de la chaîne de blocs par les organismes officiels, les inventeurs pourraient utiliser la technologie pour enregistrer une empreinte* de la description de leur brevet sur la chaîne de blocs, qui pourrait ensuite constituer la première étape du processus de demande de brevet (Boucher, 2017).

Des sociétés du secteur privé se penchent déjà sur la question pour développer des solutions à cet effet. Bernstein Technologies, une société basée à Munich, par exemple, permet aux entreprises de conserver une trace numérique des enregistrements de leurs processus d'innovation grâce à la technologie de la chaîne de blocs. Les inventions, les dessins et modèles et les preuves d'utilisation sont enregistrés sur la chaîne de blocs et un certificat de la chaîne de blocs apporte la preuve de la titularité, de l'existence et de l'intégrité de tout actif quelconque de propriété intellectuelle.⁵⁶ Les renseignements enregistrés restent privés grâce à la cryptographie.

Même si ces solutions pourraient apporter des améliorations précieuses en termes d'efficacité, la chaîne de blocs ne modifiera pas la façon dont les brevets sont accordés. Plus que l'enregistrement effectif des brevets, c'est la gestion et le respect des droits de brevet – et des DPI en général – que la chaîne de blocs a le potentiel de transformer.

(b) Simplification de la gestion et du respect des DPI

Au-delà de la preuve de création, d'utilisation, de titularité et d'enregistrement, la technologie de la chaîne de blocs offre des possibilités particulièrement intéressantes en termes d'administration des DPI, de contrôle de leur utilisation et de moyens de les faire respecter.

Cela est particulièrement important pour le droit d'auteur, dont la gestion peut être complexe. Il peut non seulement être difficile d'apporter la preuve de la titularité, mais aussi de garder la trace des utilisateurs de l'œuvre, tandis que les tierces parties qui souhaitent utiliser une œuvre éprouvent parfois des difficultés pour savoir à qui s'adresser pour obtenir une licence. Une fois que des créations ont été téléchargées sur Internet, il devient extrêmement difficile pour les auteurs et les artistes interprètes ou exécutants de suivre les utilisations qui en sont faites et d'obtenir une rémunération pour celles-ci.

(i) Facilitation du suivi et de la concession de licences

L'utilisation de la chaîne de blocs pourrait faciliter le suivi et le contrôle de la distribution de la propriété intellectuelle enregistrée et non enregistrée par les détenteurs de DPI. Des plates-formes de chaînes de blocs telles que Binded et Ascribe, par exemple, permettent aux auteurs, une fois qu'une œuvre en ligne est enregistrée, d'effectuer des recherches dans tout un ensemble de sources afin de vérifier qui utilise leur œuvre.

La chaîne de blocs pourrait également faciliter la concession de licences aux différentes parties et la cession de droits via un logiciel, et il est possible d'imaginer un système dans lequel les transactions relatives à la concession de licences et à la cession de DPI sont introduites dans une chaîne de blocs afin de conserver un registre immuable de ces transactions et d'aider à suivre leur utilisation.

La startup Ascribe, par exemple, offre la possibilité de transférer, de consigner ou de prêter des créations numériques via sa plate-forme basée sur la chaîne de blocs, ainsi que de suivre leur utilisation. Dans le cas des marques de fabrique ou de commerce, les entrées introduites dans la chaîne de blocs pourraient alors constituer une preuve d'utilisation de la marque de fabrique ou de commerce. Un autre exemple est KodakOne, une plate-forme de chaîne de blocs qui permet aux photographes et aux agences de stocker leurs images et les métadonnées connexes et de suivre les transactions relatives à la titularité, aux droits et aux licences, indépendamment du point de savoir où ces images sont utilisées et par qui.⁵⁷

(ii) DPI intelligents

L'une des caractéristiques les plus intéressantes de la technologie est la possibilité d'utiliser des contrats intelligents qui s'exécutent automatiquement si certaines conditions sont remplies. Des contrats intelligents construits sur une chaîne de blocs pourraient s'avérer particulièrement utiles pour garantir une rémunération automatique, flexible et équitable des détenteurs des droits.

Dans l'industrie musicale, par exemple, où le suivi de l'utilisation des œuvres créatives est un problème particulièrement sensible, il est possible d'imaginer qu'un auteur de chansons pourrait mettre dans la chaîne de blocs une chanson accompagnée d'un contrat intelligent qui préciserait les coordonnées du ou des détenteurs des droits et les conditions applicables à l'utilisation de l'œuvre. Cela faciliterait la mise en relation des tierces parties avec le ou les détenteurs des droits en vue d'obtenir une licence pour l'utilisation de leur œuvre, et l'obtention d'une rémunération par l'auteur de la chanson et les autres détenteurs des droits pour l'utilisation de leurs créations. Les licences accordées par l'intermédiaire de contrats intelligents s'appliqueraient directement dès l'utilisation de l'œuvre. Le paiement des redevances s'exécuterait automatiquement et les montants des redevances facturés pourraient être flexibles et adaptés en fonction de l'usage (les utilisateurs fréquents, par exemple, pourraient payer moins que les utilisateurs ponctuels).

Des arrangements de ce type existent en fait déjà; par exemple, la chanteuse Imogen Heap, artiste britannique de studio d'enregistrement à succès et fondatrice de Mycelia, un site de recherche-développement destiné aux musiciens, a lancé en 2017 un projet pilote avec Featured Artists Coalition (FAC) et Digital Catapult

faisant intervenir la technologie de la chaîne de blocs. Le projet pilote, qui portait sur deux chansons d'Imogen Heap au moment de la rédaction, permet aux utilisateurs d'acheter des licences pour télécharger, écouter en flux continu et mixer les chansons via des contrats intelligents. Les paiements sont automatiquement envoyés à tous les détenteurs de droits au moment de l'utilisation des chansons. S'appuyant sur l'expérience du projet pilote, Mycelia élabore désormais un passeport créatif (« Creative Passport ») pour permettre aux musiciens intéressés d'utiliser la technologie pour automatiser et personnaliser la gestion de leurs droits de propriété intellectuelle. L'objectif du projet de passeport créatif de Mycelia est de créer un « écosystème de l'industrie musicale équitable, durable et dynamique » dans lequel toutes les parties participantes, des musiciens aux distributeurs, sont rémunérés équitablement pour leur travail.⁵⁸ La chaîne de blocs « pourrait aider les musiciens à gagner de nouveau de l'argent », comme l'indique Imogen Heap (Heap, 2017).

L'utilisation de la chaîne de blocs peut-elle conduire à une décentralisation complète de la gestion du droit d'auteur et menacer des intermédiaires bien établis tels que les labels et les maisons de disque, les organismes de gestion des droits d'exécution et les services de diffusion numérique en flux continu tels que Spotify ? Rien n'est moins sûr. Ces intermédiaires jouent un rôle important en matière de commercialisation et de gestion qu'un registre distribué ne peut pas remplir à l'heure actuelle. En outre, il est probable qu'ils résisteront et lutteront contre toute tentative visant à les marginaliser.

En fait, conscients des enjeux, trois des plus grandes sociétés de concession de licences et de perception des redevances – l'ASCAP (États-Unis), la SACEM (France) et PRS for Music (Royaume-Uni) – ont uni leurs forces en avril 2017 pour élaborer un prototype d'enregistrement et de gestion des métadonnées utilisant la chaîne de blocs d'IBM pour faciliter la détermination de la titularité et accélérer la concession de licences et le versement des redevances (Smirke, 2017). Ce même mois, la société de diffusion de musique en flux continu Spotify a fait l'acquisition de Mediachain Labs⁵⁹, une startup qui élabore des solutions basées sur la chaîne de blocs afin de résoudre les problèmes d'attribution des droits. Grâce à cette acquisition, Spotify espère mieux relier les artistes et les autres détenteurs de droits aux pistes hébergées sur son service et contribuer à résoudre les problèmes d'attribution de la musique (Higgins, 2017b). Cette évolution semble laisser entendre qu'il est probable que le secteur restera consolidé, et que nous sommes davantage susceptibles d'assister à une réorganisation qu'à une révolution.

La chaîne de blocs pourrait également être un outil intéressant pour gérer la « titularité partagée », c'est-à-dire les droits appartenant à différents détenteurs, une situation qui est devenue relativement courante de nos jours, en particulier dans

l'industrie musicale, comme nous l'avons vu précédemment, et pour les innovations brevetées. Dans le cas des brevets, bien souvent, l'innovation n'a plus lieu en interne. La collaboration entre plusieurs individus et entités est devenue la norme, ou presque, ce qui fait de la gestion des droits de brevet un exercice plus complexe. La chaîne de blocs pourrait aider à enregistrer et à suivre dans quelle mesure chacun a apporté une contribution, à déterminer qui obtiendra des parts des futures recettes et à garantir la rémunération automatique des divers détenteurs des droits.

C'est également vrai des savoirs traditionnels. Le système actuel de protection conférée par des brevets a été élaboré « à l'âge de l'industrialisation en Occident et développé par la suite en fonction des besoins perçus des sociétés avancées sur le plan technologique », comme le note l'OMPI sur son site Web.⁶⁰ Pendant plusieurs décennies, les peuples indigènes et les communautés locales dans les pays en développement ont fait valoir que les savoirs traditionnels, c'est-à-dire l'ensemble vivant de connaissances développées et transmises d'une génération à l'autre au sein d'une communauté, qui font souvent partie de son identité culturelle ou spirituelle, tels que les médicaments traditionnels, devraient se voir accorder une protection effective, et que les autorités des pays tiers devraient veiller à ce que les déposants de demandes de brevets aient eu un accès autorisé de la part des autorités nationales aux ressources génétiques et aux savoirs traditionnels avant d'accorder un brevet. En Inde, où les savoirs traditionnels jouent un rôle essentiel, une base de données consultable de médicaments traditionnels – qui n'est pas basé sur la chaîne de blocs – a été établie et peut être utilisée comme preuve de l'état de la technique par les examinateurs de brevet lorsqu'ils évaluent les demandes de brevet. Le caractère mondial, immuable et transparent de la chaîne de blocs, associé à la possibilité d'utiliser les contrats intelligents pour automatiser les paiements, pourrait aider ces communautés à monétiser la valeur de leurs savoirs de façon plus fiable et à suivre l'utilisation qui en est faite.

Comme ces exemples le montrent, la chaîne de blocs peut faciliter le contrôle et le suivi de la distribution de la propriété intellectuelle enregistrée et non enregistrée, simplifier la concession de licences et la cession de droits, aider à gérer les droits, à accélérer et optimiser le paiement des redevances et à garantir un dédommagement équitable des détenteurs de droits; et, ce, à l'échelle mondiale.

(iii) Vers des « chaînes mondiales de propriété intellectuelle » ?

Nous vivons dans une économie mondialisée, mais il n'existe pas de brevet, de marque de fabrique ou de commerce ni de droit d'auteur mondiaux. Les DPI gardent un caractère territorial. Dans ce contexte, la gestion des DPI peut être un exercice particulièrement complexe. L'utilisation combinée de la chaîne de blocs et des contrats intelligents pourrait, à cet égard, offrir de nouvelles possibilités. Les contrats

intelligents pourraient faciliter la gestion des DPI à l'échelle mondiale, et contribuer ainsi à l'émergence de « chaînes mondiales de propriété intellectuelle ».

Dans le domaine du droit d'auteur, par exemple, la complexité de la concession de licences de droit d'auteur dans un environnement transfrontières, dans lequel les lois sur le droit d'auteur sont largement nationales, a conduit à l'élaboration des projets de code source ouvert⁶¹ et creative commons.⁶² Il est souvent trop onéreux pour un détenteur ordinaire de droits d'engager un conseil juridique qualifié pour tenir compte de la diversité des lois existantes en vue de conclure des accords de licences transfrontières. Les projets de code source ouvert et creative commons ont permis de contourner ce problème en rendant l'œuvre librement accessible en ligne et en permettant à toute personne de l'utiliser ou de l'améliorer sans avoir l'obligation de verser une compensation financière quelconque, sous réserve que le créateur de l'œuvre soit reconnu comme créateur. Dans le cadre de cette approche, les œuvres ont une portée mondiale, mais leurs créateurs ne sont pas rémunérés.

L'utilisation de contrats intelligents conjointement avec la chaîne de blocs pourrait résoudre le dilemme des licences libres/creative commons en permettant d'occulter le caractère territorial du droit d'auteur tout en rendant possible, dans le même temps, le paiement équitable et automatique de redevances de licences au(x) créateur(s) de l'œuvre (Savelyev, 2017). Des approches similaires pourraient être envisagées pour d'autres types de DPI.

Un certain nombre de personnes ont également spéculé que la chaîne de blocs pourrait donner lieu à des registres mondiaux des DPI, ce qui améliorerait la visibilité et la transparence des « chaînes de DPI » à l'échelle mondiale. Les renseignements sur les DPI demeurent dispersés. Le système actuel de brevets consiste en quelque 200 offices nationaux et régionaux indépendants. C'est également le cas pour les marques de fabrique ou de commerce et le droit d'auteur. Plusieurs tentatives ont été faites pour créer des registres mondiaux dans le domaine du droit d'auteur, mais elles ont échoué. En 2008, l'Union européenne a tenté de créer une base de données des œuvres musicales mondiales (« Global Repertoire Database »), mais le projet a été stoppé après que les sociétés de gestion des droits d'auteur et les éditeurs ont refusé de le soutenir. D'autres projets, tels que le registre international de la musique (« International Music Registry »), soutenu par l'OMPI, ont connu le même sort.

Le caractère décentralisé de la chaîne de blocs peut-il ouvrir de nouvelles perspectives à cet égard ? Il est possible d'imaginer la création de registres mondiaux propres à la propriété intellectuelle reliant tous les registres nationaux et toutes les parties prenantes pertinentes. Les renseignements ajoutés à un registre de la propriété intellectuelle basé sur la chaîne de blocs seraient accessibles à tous,

mais seules les autorités nationales ou les autres parties prenantes pertinentes seraient en mesure d'écrire dans la chaîne de blocs.

Même si cela est possible en théorie, ces initiatives pourraient se heurter aux mêmes obstacles que les précédentes tentatives dans le domaine du droit d'auteur. Elles nécessiteraient l'engagement et la volonté politique de tous les participants, ainsi que d'importants efforts de coordination. Bien que ce ne soit pas impossible, ce ne sera pas un exercice facile, d'autant que des limitations techniques affectent encore la technologie elle-même. L'élan viendra peut-être du secteur privé; plusieurs startups travaillent déjà sur des initiatives de ce type. Par exemple, la startup IPwe⁶³ aspire à créer un registre mondial des brevets (« Global Patent Registry ») basé sur la chaîne de blocs et plusieurs startups ont formé le consortium Concensum en vue d'établir un registre mondial des droits d'auteur (« Global Copyright Register »).⁶⁴

Le point de savoir si ces initiatives, qui en sont encore à leurs balbutiements, réussiront à apporter une plus grande transparence au paysage des DPI reste à démontrer, mais elles ont le mérite de mettre la question de la transparence mondiale des DPI sur la table. Il reste aussi à savoir si les juridictions nationales souhaiteront reconnaître comme valides des DPI introduits dans une chaîne de blocs.

Une chose est sûre : le caractère disruptif de la chaîne de blocs, les possibilités que la technologie ouvre, ainsi que ses implications juridiques potentielles méritent l'attention des organismes de réglementation et des législateurs.

(iv) Lutte contre le piratage et la contrefaçon

En avril 2018, le musée français Terrus, consacré au peintre Etienne Terrus, un ami proche du peintre Henri Matisse, a découvert que plus de la moitié de sa collection était constituée de faux (France24, 2018). Les produits contrefaits sont légion et affectent de la même manière tous les domaines de la propriété intellectuelle – œuvres artistiques et créatives, inventions et marques. La chaîne de blocs offre des possibilités intéressantes lorsqu'il s'agit de lutter contre le piratage et la contrefaçon, le caractère immuable et transparent de la chaîne de blocs permettant de vérifier facilement l'origine des produits. Les empreintes d'œuvres de propriété intellectuelle numérisables, telles que les livres, sur la chaîne de blocs peuvent servir de preuve d'existence et d'origine, tandis que l'utilisation concomitante de la chaîne de blocs et des contrats intelligents peut permettre aux détenteurs de DPI de contrôler et de suivre l'utilisation appropriée de leurs DPI comme discuté plus haut.

S'agissant des objets matériels, un code QR* lisible par scanner apposé sur une œuvre ou un produit peut donner accès à l'historique de l'œuvre ou du produit et servir à prouver son authenticité. De multiples startups élaborent des solutions pour

suivre et identifier des produits tels que les produits pharmaceutiques, les produits électroniques et les articles de luxe et de mode, et veiller à ce que les consommateurs ou les producteurs reçoivent un produit authentique. Everledger pour les diamants, Blockpharma pour les produits pharmaceutiques, ainsi que Blockverify, VeChain et Chronicled pour la protection contre la contrefaçon d'un éventail de produits sont certaines des sociétés actives dans ce domaine. La marque de mode Babyghost, par exemple, s'est associée avec VeChain, une startup qui se concentre sur la protection des marques, des marques de fabrique ou de commerce et des produits, en incorporant dans chaque vêtement une puce VeChain comportant une clé publique stockée sur la chaîne de blocs.

En scannant le code QR de l'étiquette avec leur smartphone, les consommateurs peuvent accéder à l'historique du vêtement, y compris aux renseignements sur le designer et le modèle, et vérifier l'authenticité du produit (voir aussi la section 4.1 a) et Campbell, 2016). Dans la plupart des cas, le potentiel de la chaîne de blocs est réalisé grâce à l'utilisation d'autres technologies et innovations, en particulier l'Internet des objets.

Il est facile d'imaginer les possibilités que les chaînes de blocs ouvrent en matière de lutte contre la contrefaçon dans le commerce international. L'Accord sur les ADPIC donne aux Membres de l'OMC la possibilité d'autoriser les fonctionnaires des douanes à agir de leur propre initiative, d'office, pour suspendre la mise en libre circulation des marchandises pour lesquelles il existe des éléments de preuve qu'elles portent atteinte à des DPI.⁶⁵ Un problème clé est le manque d'expertise de la plupart des fonctionnaires des douanes en matière de détection de marchandises contrefaites.

L'utilisation de la technologie pour retracer la provenance des produits, de l'usine aux utilisateurs finals, pourrait s'avérer utile pour démontrer qu'il existe des éléments de preuve *prima facie* d'une atteinte à des droits. Le titulaire d'une marque utilisant la technologie de la chaîne de blocs pour consigner l'historique de ses produits pourrait, par exemple, informer les services des douanes et les organismes chargés de faire respecter les droits que ses produits incluent une étiquette cryptographique liée à la chaîne de blocs qui atteste de son origine. L'absence d'étiquette ou une étiquette incorrecte faciliterait la détection des contrefaçons par les fonctionnaires chargés de faire respecter les droits (Burstall et Clark, 2017).

Les enjeux sont élevés, non seulement dans les domaines tels que ceux des produits pharmaceutiques et des produits de luxe, mais aussi dans l'industrie automobile et l'aéronautique, secteurs dans lesquels, comme dans celui de la santé, les contrefaçons peuvent être très dangereuses.

Toutefois, le fait que la chaîne de blocs pourrait rendre le respect des DPI, en particulier du droit d'auteur, quasi impossible pour les produits numériques inquiète de plus en plus. En effet, si les données enregistrées dans une chaîne de blocs ne peuvent pas être facilement altérées, rien n'empêche un utilisateur malveillant de présenter une version pirate d'une œuvre à la chaîne de blocs – et rien n'oblige le contrevenant à joindre au téléchargement un type quelconque de données d'identification. Le caractère décentralisé et anonyme des chaînes de blocs publiques fait qu'il est extrêmement difficile, voire impossible, d'identifier ceux qui achètent et vendent des copies non autorisées de produits numériques et de leur en attribuer la responsabilité (Vogel, 2015; Gabison, 2016).

Bien que la technologie présente des caractéristiques intéressantes, puisqu'elle est susceptible de faciliter le contrôle et le suivi de la distribution de la propriété intellectuelle enregistrée et non enregistrée et la lutte contre le piratage et la contrefaçon, de simplifier la concession de licences et la cession des droits et de permettre de gérer les DPI à l'échelle mondiale, ainsi que d'accélérer et d'optimiser le paiement des redevances pour garantir une compensation équitable des détenteurs de droits, ses implications pratiques et juridiques complètes doivent encore être soigneusement évaluées. Les autorités de réglementation et les législateurs devraient commencer à se pencher sur ces aspects; le plus tôt sera le mieux.

4. Amélioration des procédures de passation des marchés publics

Pour remplir leurs fonctions, les organismes publics ont souvent besoin d'acheter des marchandises et des services en utilisant les ressources publiques. Ces achats sont communément appelés marchés publics.

Les marchés publics sont un aspect essentiel du commerce international. Ils constituent un marché important, qui représente en moyenne 10 à 15% du produit intérieur brut (PIB) d'une économie, tandis que les marchés publics mondiaux représentent environ 9 500 milliards de dollars EU par an.⁶⁶

Compte tenu de l'importance économique des marchés publics, les économies qui peuvent être réalisées grâce à des procédures plus transparentes et plus efficaces peuvent avoir un impact notable sur l'économie d'un pays – en particulier en aidant à lutter contre la corruption et la fraude qui, selon les estimations, représentent entre 20 et 25% des budgets des marchés passés dans un secteur tel que la construction et près de 60% des affaires de corruption d'agents publics étrangers faisant l'objet de poursuites dans le cadre de la Convention de l'OCDE sur la lutte contre la corruption (OCDE, 2016). Une étude de 2004 de la Commission européenne a

montré qu'une économie de 10% dans le domaine des marchés publics transformerait les déficits budgétaires de certains États membres de l'UE en excédents, et ferait qu'aucun État membre de la zone euro n'afficherait de déficit du secteur public dépassant la limite de 3% (Commission européenne, 2004).

La nécessité d'une transparence et d'une efficacité accrues a incité les organismes publics du monde entier, souvent avec le soutien d'organisations multilatérales telles que la Banque mondiale et la Banque asiatique de développement (BAsB), à exploiter les technologies de l'information pour améliorer la transparence, réduire les coûts et mieux gérer et surveiller les procédures de passation des marchés publics. Après le Canada et son initiative d'administration en ligne MERX, qui a vu le jour en 1991, des systèmes de passation électronique des marchés publics – c'est-à-dire des systèmes électroniques conçus pour gérer certaines étapes, voire toutes, du processus de passation des marchés publics – ont été élaborés et lancés dans le monde entier. L'utilisation des marchés publics électroniques est désormais largement répandue, et les systèmes deviennent de plus en plus sophistiqués (Banque asiatique de développement, 2013).

Bien que le degré de sophistication varie d'un système à l'autre, les fonctionnalités généralement disponibles sont notamment les suivantes : registres des acheteurs/vendeurs; services d'information (accès aux renseignements liés aux marchés publics telles que nouvelles et publications); systèmes d'appel d'offres électroniques, qui facilitent la transmission des dossiers d'appel d'offres et permettent aux vendeurs de présenter leurs offres; enchères électroniques et enchères électroniques inversées (concurrence par les prix menée en ligne de façon dynamique); outils d'achats électroniques (pour les transactions de faible valeur portant sur de gros volumes); systèmes de commande par catalogue; cartes d'achat; et systèmes de paiements électroniques et de reçus électroniques (Banque asiatique de développement, 2013).

En parallèle, de nouveaux cadres réglementaires ont été élaborés pour permettre aux entités contractantes de tirer profit des moyens électroniques tels que la Loi type de 2011 de la CNUDCI sur la passation des marchés publics et l'Accord de l'OMC sur les marchés publics (AMP) révisé.⁶⁷

L'AMP révisé, qui est entré en vigueur en avril 2014, reconnaît qu'il est important d'utiliser des moyens électroniques et d'encourager l'utilisation de tels moyens. L'AMP énonce de façon explicite que les entités contractantes peuvent accepter les offres présentées par voie électronique – ce qui ouvre potentiellement la voie à l'utilisation de la technologie de la chaîne de blocs – mais que les systèmes et programmes informatiques pertinents doivent être «généralement disponibles etinteropérables avec d'autres systèmes et programmes informatiques généralement

disponibles»⁶⁸ – ce qui, en l'état actuel de la technologie reste un défi (voir la section 4.2 a)).

Une deuxième caractéristique intéressante de l'AMP est l'inclusion d'une référence explicite à la corruption dans son préambule : les parties à l'AMP sont tenues de mener leurs activités de passation des marchés «d'une manière transparente et impartiale» et de manière à ce que «les conflits d'intérêts et les pratiques frauduleuses soient évitées» – ce qui est une première dans un Accord de l'OMC.⁶⁹

La chaîne de blocs peut-elle être exploitée pour améliorer davantage les procédures de passation des marchés publics ? Peut-elle apporter quelque chose à des systèmes de passation des marchés publics électroniques déjà sophistiqués ? Diverses caractéristiques clés de la technologie en font un outil intéressant à utiliser dans le domaine des marchés publics, mais il est essentiel de peser soigneusement les avantages et les inconvénients.

D'abord, la chaîne de blocs fournit un environnement électronique très sûr dans lequel les données sont horodatées et stockées de façon quasi immuable. L'un des éléments les plus importants de la passation électronique des marchés publics est la sécurité. Les offres de prix commerciales présentées par les soumissionnaires doivent être stockées de façon sûre et sécurisée et, parce que les appels d'offres forment la base d'un contrat juridique, toutes les données doivent rester sûres, complètes et vérifiables. La question de la sécurité des données et de la fraude, bien que probablement moins courante que dans un environnement basé sur le papier, aurait un effet dissuasif sur la passation électronique des marchés publics (Banque asiatique de développement, 2013).

Ensuite, la chaîne de blocs permet l'automatisation des procédures de passation des marchés publics via l'utilisation de contrats intelligents, ce qui garantit l'efficacité, la neutralité et l'équité des processus. Les contrats intelligents, c'est-à-dire des contrats qui s'exécutent automatiquement stockés sur la chaîne de blocs, peuvent contribuer à améliorer tant le processus d'appel d'offre lui-même que la gestion des marchés adjugés. En effet, non seulement il est quasiment impossible pour toute partie de manipuler les données stockées, mais personne ne peut contourner le contrat intelligent et sa logique de permissions. L'automatisation des offres, des examens et des paiements, et la quasi impossibilité de manipuler les données peut contribuer à prévenir la fraude de la part des acteurs impliqués dans le processus et à réduire les coûts, et à faire en sorte que le processus soit loyal, efficace et impartial, comme le prescrit l'AMP.

Comment fonctionnerait un processus d'appel d'offres basé sur la chaîne de blocs ? Un organisme public – l'entité contractante – publierait un avis de marché envisagé.

Les fournisseurs intéressés présenteraient leur offre via l'application de chaîne de blocs utilisée par l'organisme dans le délai imparti (registre avec permission). Les offres seraient « hachées » et cryptées* au moment où elles sont présentées. À l'issue de la période de présentation des offres, toutes les offres seraient analysées et évaluées par le contrat intelligent sur la base des critères codés, et une offre retenue serait identifiée. Une fois le soumissionnaire retenu identifié, les signataires autorisés examineraient les documents présentés par le fournisseur retenu et les valideraient. L'offre retenue serait annoncée officiellement et les fournisseurs non retenus seraient automatiquement informés.

Une fois le marché adjugé, un contrat intelligent pourrait établir les conditions de livraison, d'exécution du marché et de paiement. Les travaux pourraient être vérifiés par les signataires autorisés et les marchandises fournies dans le cadre du marché seraient automatiquement enregistrées dans la chaîne de blocs via un système logistique basé sur celle-ci. Lorsque les conditions spécifiées dans le contrat intelligent seraient remplies, le paiement en faveur du fournisseur serait effectué automatiquement.

Enfin, l'utilisation de la chaîne de blocs pour mener des processus d'appel d'offre peut être particulièrement intéressante pour contribuer à satisfaire à une autre prescription de l'AMP révisé, à savoir la traçabilité électronique. L'AMP révisé prescrit aux parties d'utiliser des moyens électroniques pour assurer la traçabilité requise de la passation des marchés couverts par voie électronique pendant une période d'au moins trois ans.⁷⁰ Cette disposition vise à garantir la disponibilité des données pendant un certain laps de temps en cas de litige. Compte tenu du caractère immuable de la chaîne de blocs, l'utilisation d'un registre distribué pour mener des procédures de passation des marchés garantit de fait que toutes les données resteront accessibles aux utilisateurs autorisés automatiquement et indéfiniment.

Plusieurs pays examinent actuellement le potentiel de la chaîne de blocs dans le domaine des marchés publics. L'Administration des services généraux des États-Unis, par exemple, travaille à l'élaboration, avec des sociétés spécialisées (Sapient Consulting et United Solutions), d'une preuve de concept en vue de raccourcir la durée du processus d'examen accéléré pour les contrats informatiques grâce à l'automatisation, et de ramener le nombre de jours nécessaires à « un nombre à un chiffre » (Friedman, 2017). Le Japon teste actuellement un système basé sur la chaîne de blocs pour traiter les appels d'offres publics afin d'améliorer l'efficacité des procédures de passation des marchés publics. Le système relierait les divers offices gouvernementaux participant à un appel d'offre afin de faciliter le partage de données (Tian, 2017). Le Mexique a récemment lancé une initiative pour déployer la chaîne de blocs dans le secteur public, y compris pour les processus

d'appel d'offres.⁷¹ Les Émirats arabes unis souhaitent que l'ensemble de leur administration repose sur la technologie de la chaîne de blocs d'ici à 2020, ce qui ferait de Dubaï la première « ville construite sur la chaîne de blocs » (Lohade, 2017).

Si la chaîne de blocs semble prometteuse en termes d'amélioration des procédures de passation des marchés publics, de gestion des marchés publics et de lutte contre la fraude, il reste à savoir si ces preuves de concept sont concluantes et si l'utilisation de la chaîne de blocs peut mener la passation électronique des marchés publics vers un niveau plus sûr et plus automatisé à un coût qui justifie le passage à un système basé sur la chaîne de blocs. L'utilisation de contrats intelligents dans les procédures de passation des marchés publics demandera aussi que les questions de responsabilité soient clarifiées (voir la section 4.2 c)), et il faudra régler les questions d'interopérabilité avant que les parties à l'AMP de l'OMC ne puissent mettre en place des systèmes de ce type.

Comme les divers exemples présentés dans ce chapitre le montrent, la chaîne de blocs offre des possibilités intéressantes en termes d'amélioration de l'efficacité des transactions commerciales internationales faisant intervenir de multiples acteurs dans divers domaines visés par l'OMC, y compris le financement du commerce, les procédures à la frontière, le transport et la logistique, les services financiers, l'assurance, la distribution de détail, la propriété intellectuelle et les marchés publics, tout en fournissant un environnement sûr. Elle peut améliorer la transparence, faciliter le suivi des transactions et accélérer les processus, y compris grâce à l'utilisation de contrats intelligents, qui permettent l'automatisation des transactions. Par conséquent, elle est considérée par beaucoup comme la technologie la plus prometteuse pour numériser le commerce.

Le nombre d'applications de la chaîne de blocs liées au commerce – élaborées par des sociétés établies et des startups, qui travaillent souvent main dans la main de manière collaborative dans un environnement qui pourrait être qualifié de « concurrence coopérative », ainsi que par les autorités gouvernementales – a augmenté de manière rapide ces dernières années, non sans raison : la technologie ne pourra fonctionner à son plein potentiel que si les différentes dimensions du commerce international, du financement du commerce aux opérations douanières en passant par la logistique, sont numérisées et si des approches et des normes communes sont élaborées.

Le commerce intelligent nécessite plus que la simple technologie. Il requiert une normalisation et un environnement réglementaire propice, ce qui demande une approche holistique, coopérative, qui casse les cloisonnements existants.

Même si la chaîne de blocs présente des caractéristiques intéressantes, ce n'est pas la panacée pour tous les problèmes et il est essentiel que les coûts et les avantages soient soigneusement examinés. Pour l'instant, l'investissement dans la technologie est un pari, mais un pari que de nombreuses sociétés jugent important de relever au vu des enjeux qu'il représente.

Note de fin

1. Une transaction à compte ouvert est une vente dans le cadre de laquelle les marchandises sont expédiées et livrées avant que le paiement ne soit exigible.
2. Les lettres de crédit sont une garantie de paiement délivrée au vendeur par la banque de l'acheteur au nom de celui-ci. La lettre de crédit est un engagement écrit prévoyant que les marchandises seront réglées une fois livrées, sous réserve que les obligations liées à la lettre de crédit (c'est-à-dire les conditions de livraison et la présentation de documents tels que les connaissements, qui énumèrent et détaillent les marchandises expédiées) soient remplies. La lettre de crédit est une garantie prévoyant que la banque s'acquittera de la somme due, dans le cas où l'acheteur serait dans l'incapacité de payer.
3. Le rapport annuel «Rethinking Trade & Finance» de la Commission bancaire de la Chambre de commerce internationale (ICC) fait état de «la disparition annoncée de longue date de la lettre de crédit documentaire». Près de 80% des répondants s'attendent à un accroissement faible ou nul de l'utilisation du financement traditionnel du commerce dans les années à venir, voire à un déclin. Voir Chambre de commerce internationale (ICC) (2017a).
4. Voir le Guide pratique relatif à la facilitation du commerce de la CEE-ONU pour de plus amples renseignements : <http://tfig.unece.org/FR/contents/open-accounts.htm>.
5. Les banques participantes sont les suivantes : Banco Santander, Deutsche Bank, HSBC, KBC, Natixis, Nordea, Rabobank, Société Générale et Unicredit.
6. Voir <https://www.ibm.com/blogs/blockchain/2017/03/disrupting-supply-chain-financing-mahindra/>.
7. Voir <https://www.hyperledger.org/news/2017/04/11/4-11-17-coinspeaker-ibm-and-sichuan-hejia-launched-a-blockchain-platform-for-pharmaceutical-procurement>.
8. Voir <https://www.dianrong.com/en/news/desktop/58d0ea009578922900e60d02.html>.
9. Certains projets basés sur la chaîne de blocs sont spécifiquement axés sur les processus de connaissance du client, tels que la plate-forme partagée de connaissance du client mise au point par IBM en coopération avec la Deutsche Bank, HSBC, Mitsubishi UFJ Financial Group (MUFG) et les centrales de trésorerie de Cargill. Voir <http://fintechnews.sg/14420/blockchain/ibm-completes-poc-blockchain-based-shared-kyc-deutsche-bank-hsbc-mufg-cargill-ibmtreasures/>.
10. Voir <https://www.r3.com/>.
11. Voir https://www.wto.org/french/news_f/brief_tradef_a_f.htm.
12. FAO/CIPV, Fiche d'information e-Phyto n° 7. Disponible à l'adresse suivante : https://www.ippc.int/static/media/files/publication/fr/2017/11/IPPC_ePhyto_Factsheet7_ib_W.pdf.
13. CEE-ONU, Recommandation n° 33.
14. Article 10:4 de l'Accord.
15. Voir <https://www.youtube.com/watch?v=tdhpYQCWnCw&feature=youtu.be>.
16. Si les marchandises sont envoyées vers une destination différente, les prescriptions peuvent différer et un nouveau certificat peut être nécessaire.

17. En décembre 2017, l'Office national philippin de l'alimentation (NFA) a publié une mise en garde au sujet d'individus ou d'entités utilisant des permis d'importation falsifiés ou contrefaits pour le riz à la suite d'un rapport indiquant que certains individus ou parties sans scrupule vendaient de faux permis soi-disant délivrés par le NFA. Voir <http://www.nfa.gov.ph/35-news/1053-nfa-warns-against-fake-rice-import-permits>. Adresse consultée le 20 juin 2018.

18. Les décisions anticipées sont des décisions contraignantes émanant des autorités douanières. Ces décisions peuvent être demandées par les importateurs ou les exportateurs au sujet de la classification, de l'origine ou de la valeur en douane des marchandises destinées à être importées ou exportées. Les décisions anticipées sont contraignantes sur l'ensemble du territoire douanier et sont valables pour une durée déterminée. Les décisions anticipées facilitent le processus de mainlevée et de dédouanement, car elles garantissent que certaines évaluations clés ont déjà été effectuées. L'article 3 de l'AFE énonce des disciplines spécifiques sur les décisions anticipées.

19. L'article 7:1 de l'AFE dispose ce qui suit «[c]haque Membre adoptera ou maintiendra des procédures permettant de présenter les documents relatifs à l'importation et les autres renseignements requis, y compris les manifestes, pour commencer le traitement avant l'arrivée des marchandises en vue d'accélérer la mainlevée de celles-ci à l'arrivée». Ce même article encourage le dépôt des documents sous forme électronique pour le traitement avant arrivée de ces documents, ouvrant la voie à l'utilisation de technologies telles que la chaîne de blocs pour traiter les documents douaniers (paragraphe 1.2 de l'article 7).

20. L'article 7:8 de l'AFE prescrit aux Membres de l'OMC «[d'adopter] ou de [maintenir] des procédures permettant la mainlevée accélérée au moins des marchandises entrées par des installations de fret aérien aux personnes qui demanderont un tel traitement, tout en maintenant le contrôle douanier».

21. L'article 7:4 de l'AFE prescrit aux Membres de l'OMC de «fonder[] la gestion des risques sur une évaluation des risques reposant sur des critères de sélection appropriés» de manière à «éviter toute discrimination arbitraire ou injustifiable ou toute restriction déguisée au commerce international». Les critères de sélection «pourront inclure, entre autres, le code du Système harmonisé, la nature et la description des marchandises, le pays d'origine, le pays de départ de l'expédition, la valeur des marchandises, les antécédents des négociants pour ce qui est du respect des exigences, et le type de moyens de transport».

22. Voir la Convention de 1990 relative à l'admission temporaire de l'OMD (http://www.wcoomd.org/-/media/wco/public/fr/pdf/about-us/legal-instruments/conventions-and-agreements/istanbul/istanbul_legal_text_fr.pdf?la=fr).

23. La DG TAXUD est la direction générale de la Commission de l'Union européenne chargée des politiques de l'UE relatives à la fiscalité et aux douanes.

24. Un carnet ATA est un document douanier international utilisé dans 87 pays qui permet l'admission temporaire en franchise de droits de la plupart des marchandises, normalement pour une durée maximale de 1 an.

25. L'article 7:5 de l'AFE dispose que «[c]haque Membre sélectionnera une personne ou un envoi aux fins du contrôle après dédouanement d'une manière fondée sur les risques, ce qui pourra inclure des critères de sélection appropriés».

26. Un opérateur agréé – ou opérateur économique agréé – est défini par l'Organisation mondiale des douanes (OMD) comme une partie intervenant dans le mouvement international des

marchandises à quelque titre que ce soit et qui a été reconnue par ou au nom d'une administration nationale des douanes comme respectant les normes de l'OMD ou des normes équivalentes en matière de sécurité de la chaîne logistique. Les critères pour pouvoir être considéré comme un opérateur agréé seront spécifiés dans les lois, réglementations ou procédures des Membres de l'OMD. Les opérateurs économiques agréés incluent des fabricants, des importateurs, des exportateurs, des courtiers, des transporteurs, des regroupements, des intermédiaires, des ports, des aéroports, des exploitants de terminaux, des opérateurs intégrés, des exploitants d'entrepôts et des distributeurs. L'article 7:7 de l'AFE inclut des dispositions spécifiques concernant l'accréditation des opérateurs agréés.

27. Voir <https://www.youtube.com/watch?v=LeKapqAQimk>.

28. Hyperledger Burrow (<https://www.hyperledger.org/projects/hyperledger-burrow>) et Hyperledger Sawtooth (<https://sawtooth.hyperledger.org/docs/core/releases/1.0/introduction.html>).

29. Entretien avec les services néerlandais des douanes. Les services néerlandais des douanes œuvrent à l'établissement d'autres circuits bilatéraux sans papier.

30. Il existe trois principaux modèles de guichets uniques :

- Ceux qui sont organisés autour d'une autorité unique qui reçoit les renseignements (sur papier ou par voie électronique), communique ces renseignements à toutes les autorités pertinentes et coordonne les contrôles pour éviter les obstacles indus dans la chaîne logistique. C'est le modèle utilisé en Suède.
- Des systèmes uniques automatisés pour la collecte et la diffusion des renseignements qui intègrent la collecte, l'utilisation et la diffusion (ainsi que le stockage) par voie électronique des données liées aux échanges qui franchissent la frontière – c'est le cas aux États-Unis. Les guichets uniques de ce type peuvent être intégrés (c'est-à-dire que les données sont traitées par l'intermédiaire du système) ou basées sur des interfaces (c'est-à-dire que les données sont envoyées à l'organisme compétent pour être traitées), ou encore une combinaison des deux.
- Des systèmes d'information et de transaction automatisés, par l'intermédiaire desquels un négociant peut présenter des déclarations commerciales électroniques aux diverses autorités pour traitement et approbation dans une seule demande. C'est le modèle le plus perfectionné de guichets uniques. Ce modèle est utilisé à Singapour.

Voir CEE-ONU, «Recommandation et lignes directrices en vue de la mise en place d'un guichet unique». Disponible à l'adresse suivante : https://www.unece.org/fileadmin/DAM/cefact/recommendations/rec33/rec33_trd352f.pdf.

31. Voir la Recommandation n° 34 de la CEFACT-ONU, «Simplification et normalisation des données pour le commerce international», décembre 2010. Disponible à l'adresse suivante : <http://tf.unece.org/FR/contents/recommendation-34.htm>.

32. D'après la page Web <http://www.fao.org/fao-who-codexalimentarius/home/fre/> le «Codex Alimentarius, ou «Code alimentaire», est un ensemble de normes, de lignes directrices et de codes d'usages adoptés par la Commission du Codex Alimentarius. La Commission a été créée par l'Organisation des Nations Unies pour l'alimentation et l'agriculture (FAO) et l'Organisation mondiale de la santé (OMS) afin de protéger la santé des consommateurs et de promouvoir des pratiques loyales en matière de commerce de denrées alimentaires».

33. En octobre 2017, le Fonds pour l'application des normes et le développement du commerce (STDF), un partenariat mondial qui aide les pays en développement à obtenir et à conserver l'accès aux marchés grâce au renforcement des capacités dans le domaine sanitaire et phytosanitaire, a approuvé un financement pour une étude de faisabilité qui examinera les options en matière de certification électronique dans le domaine vétérinaire. L'étude sera menée par l'OIE, en étroite collaboration avec la FAO, le Groupe de la Banque mondiale, l'OMD et d'autres organisations.
34. Voir <https://blockfreight.com/>.
35. Voir <https://events.sap.com/teched/en/session/36839>.
36. Voir https://www.quasa.io/src/assets/pdf/wp_en.pdf.
37. Voir, par exemple, <https://www.bloomberg.com/news/articles/2018-04-18/drowning-in-asea-of-paper-world-s-biggest-ships-look-for-a-way-out> et <https://www.supplychaindigital.com/technology/blockchain-technology-set-revolutionise-logistics-industry>.
38. Voir <https://www.tradelens.com>.
39. Voir le communiqué de presse d'IBM : <http://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution>.
40. Entretien de l'auteure avec Accenture en 2018.
41. Voir <https://bita.studio/>.
42. Cette liste ne se veut pas exhaustive. Le choix a été fait de se concentrer sur les secteurs dans lesquels les transactions transfrontières sont susceptibles d'être le plus affectées. D'autres secteurs des services, tels que le secteur de la santé et celui des services relatifs aux voyages, ont commencé à explorer l'utilisation de la chaîne de blocs pour réduire les coûts, simplifier les procédures, améliorer la coordination entre les diverses parties prenantes, améliorer l'efficacité des systèmes de réservation/de rendez-vous, etc.
43. Le réseau privé basé sur la chaîne de blocs Linq du Nasdaq, par exemple, permet à des sociétés privées d'émettre et de négocier des actions – voir Nasdaq (2015).
44. Voir <https://www.traxpay.com/>.
45. Les expressions « compte nostro » et « compte vostro » désignent la même chose considérée de points de vue différents. Si la banque A détient auprès de la banque B un compte libellé dans la monnaie nationale de la banque B, ce compte est un compte nostro pour la banque A (c'est-à-dire que, du point de vue de la banque A, le terme « nostro » désigne « notre » compte auprès de la banque B) et un compte vostro (ou « votre » compte) pour la banque B.
46. Ripple est un système de registre distribué, mais pas une chaîne de blocs proprement dite.
47. Voir <https://ripple.com/>.
48. Voir, par exemple, Deloitte (2016), Ernst & Young (2017), KPMG (2017), McKinsey & Company (2016a) et PricewaterhouseCoopers (2016).
49. À l'OMC, l'expression commerce électronique « s'entend de la production, de la distribution, de la commercialisation, de la vente ou de la livraison de marchandises et services par des moyens électroniques » (document officiel de l'OMC portant la cote WT/L/274). À l'OMC, les travaux sur le commerce électronique vont donc au-delà de la dimension services du commerce électronique. Les

questions liées au commerce des marchandises, à la propriété intellectuelle et au développement relèvent également du programme de travail de l'OMC sur le commerce électronique. La présente section se concentre exclusivement sur la distribution de détail et la dimension services du commerce électronique.

50. Voir <https://www.openbazaar.org/>.

51. Article 2 de la Convention de Berne (https://www.wipo.int/treaties/fr/text.jsp?file_id=283698).

52. Voir par exemple <https://poex.io/about>, <https://proofofexistence.com/about> et <https://www.microsoft.com/en-us/store/p/proof-of-existence/9nblggh4z1t2>.

53. Voir <https://binded.com>.

54. Voir <https://cognate.com/>.

55. Ibidem.

56. Voir <https://www.bernstein.io/>.

57. Voir <https://kodakone.com/index.php?id=1>.

58. Voir <http://myceliaformusic.org>.

59. Voir <http://www.mediachain.io/>.

60. Voir http://www.wipo.int/pressroom/en/briefs/tk_ip.html.

61. Un logiciel libre est un logiciel informatique dont le code source est communiqué dans le cadre d'une licence en vertu de laquelle le détenteur du droit d'auteur accorde aux utilisateurs le droit d'étudier, de modifier, d'améliorer et de distribuer le logiciel à toute personne et quel que soit l'objectif visé. Un code source ouvert suppose la libre accessibilité au code source et la libre distribution.

62. Le projet Creative Commons (CC) permet aux détenteurs des droits de partager de façon légale leurs connaissances et leur créativité d'une manière plus équitable, accessible et flexible. Les licences Creative Commons permettent la libre distribution d'une œuvre autrement protégée par le droit d'auteur. Une licence Creative Commons est utilisée lorsqu'un auteur souhaite donner à des personnes le droit d'utiliser, de partager et de s'inspirer d'une œuvre qu'il a créée. Ces licences sont souvent considérées comme l'«équivalent du logiciel libre» pour les œuvres non codées. Pour de plus amples renseignements, voir <https://creativecommons.org>.

63. Voir <https://ipwe.com/ipwe-registry>.

64. Voir <https://concensum.org/en/e-services>.

65. Article 58 de l'Accord sur les ADPIC.

66. Voir <https://www.open-contracting.org/why-open-contracting/>.

67. Les pratiques en matière de marchés publics ne sont pas visées par les règles multilatérales de l'OMC, mais par un accord plurilatéral qui inclut à l'heure actuelle 47 Membres (y compris l'Union européenne et ses 28 États membres – données de 2018). En fait, les marchés publics sont explicitement exemptés des principales disciplines tant de l'Accord général sur les tarifs douaniers et le commerce (GATT – voir l'article III:8 a) que de l'Accord général sur le commerce des services (AGCS – voir l'article XIII:1).

68. Article IV:3 a) de l'AMP révisé.

69. Le texte exact du Préambule est le suivant : « Reconnaissant qu'il est important que les mesures en matière de marchés publics soient transparentes, que les marchés soient passés d'une manière transparente et impartiale, et que les conflits d'intérêts et les pratiques frauduleuses soient évités, conformément aux instruments internationaux applicables tels que la Convention des Nations Unies contre la corruption » (https://www.wto.org/french/docs_f/legal_f/rev-gpr-94_01_f.htm).

70. Article XVI:3 b) de l'AMP révisé.

71. Voir https://www.unece.org/fileadmin/DAM/cefact/cf_forums/2017_Rome/PPTs/BlockChain/PM_05_Yolanda_Martinez_Mancilla_Mexico_Blockchain_HACKMX.pdf, diapositives 23 et 24.

4 Un monde de possibilités... et de défis

D'après une étude publiée par le Parlement européen en 2017, la chaîne de blocs pourrait «changer nos vies» (Boucher, 2017). Ce que montrent les différentes applications de la chaîne de blocs qui sont mises au point dans des domaines aussi divers que le financement du commerce, la facilitation des échanges, le commerce des services, la propriété intellectuelle et les marchés publics, c'est que la chaîne de blocs peut avoir un impact considérable sur les opérateurs commerciaux et sur les organismes gouvernementaux participant au commerce international. Les possibilités sont multiples, mais elles ne seront réalisées que si plusieurs défis clés sont relevés.

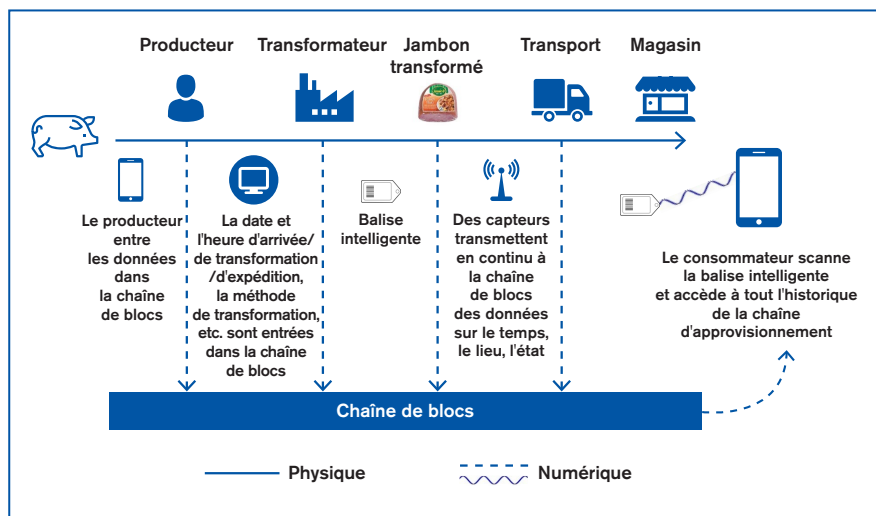
1. Des possibilités multiples

(a) Accroître la confiance et la transparence dans les chaînes de valeur

L'une des utilisations les plus évidentes de la chaîne de blocs est la surveillance des données. La chaîne de blocs, combinée à l'Internet des objets, offre de nouvelles façons de suivre le parcours des produits. C'est un outil puissant pour promouvoir la transparence et la traçabilité des chaînes d'approvisionnement (voir la figure 13), pour aider à lutter contre la contrefaçon et pour renforcer la confiance des consommateurs.

À la différence des systèmes d'étiquetage actuels, qui peuvent être manipulés, la chaîne de blocs offre un moyen très sûr de prouver l'origine et l'authenticité des produits. Le nombre de start-up et de sociétés qui l'utilisent pour faciliter le suivi des produits et la lutte contre la contrefaçon a augmenté en flèche.

L'entreprise Agridigital, par exemple, utilise la chaîne de blocs pour aider les entreprises agricoles à remédier aux inefficiences et aux risques dans la chaîne d'approvisionnement et pour suivre la provenance des produits agricoles qu'elles

Figure 13 Illustration d'un processus de traçabilité de bout en bout

Source : Auteure.

utilisent.¹ D'autres entreprises utilisent cette technologie pour offrir aux sociétés des solutions permettant d'accroître la transparence de la chaîne d'approvisionnement et de lutter contre la contrefaçon. C'est le cas de Blockverify, qui aide les entreprises à lutter contre la contrefaçon de produits pharmaceutiques, d'articles de luxe, de diamants et de produits électroniques, et de Everledger, qui leur permet d'enregistrer et de suivre le parcours des diamants depuis la mine jusqu'au magasin.

Diverses initiatives visent à accroître la transparence pour renforcer la confiance des consommateurs. Par exemple, Provenance, une start-up établie au Royaume-Uni et spécialisée dans la traçabilité de la chaîne de blocs, collabore avec Co-op, la plus grande coopérative de consommateurs du Royaume-Uni, pour suivre en temps réel le parcours des produits frais de la source jusqu'au supermarché afin d'accroître la confiance des consommateurs dans le commerce de détail des produits alimentaires. À chaque étape du parcours, des données sur le produit, le fournisseur, l'emplacement et l'impact environnemental et social de chaque entreprise, sont recueillies et ajoutées à la chaîne de blocs, ce qui crée un historique numérique du produit qui est accessible à tous, de la ferme aux consommateurs.² La multinationale française Carrefour utilise aussi la technologie de la chaîne de blocs pour améliorer la traçabilité de ses produits d'origine animale et garantir aux consommateurs la plus grande transparence possible.³ Un autre projet de Provenance, dans le secteur de la mode, a permis de suivre le parcours de la laine d'alpaga durable depuis la

tonte à la ferme jusqu'au filage, au tricotage et à la finition dans le studio de mode londonien de Martine Jarlgaard, ce qui permet aux clients de vérifier l'authenticité des matériaux utilisés et de connaître les processus et les personnes qui ont contribué à la fabrication des produits.⁴

À la suite des divers scandales qui ont secoué l'industrie alimentaire ces dernières années, les grandes entreprises alimentaires et de détail se tournent vers la chaîne de blocs pour accroître la transparence de la chaîne d'approvisionnement alimentaire, mais aussi pour pouvoir suivre rapidement les produits contaminés et rétablir la confiance dans la qualité des aliments consommés.

Par exemple, en octobre 2016, l'entreprise américaine Walmart s'est associée à IBM et à l'université Tsinghua de Beijing pour suivre le parcours de la viande de porc en Chine au moyen d'une chaîne de blocs. La chaîne de blocs collecte des renseignements sur la façon dont la viande est passée des producteurs aux transformateurs puis aux distributeurs, aux commerçants et, enfin, aux consommateurs. L'origine et le numéro de lot du produit, les renseignements sur l'usine et les méthodes de transformation, les dates de péremption et les détails sur les étapes de la vente au détail sont consignés dans la chaîne de blocs, ce qui permet de détecter rapidement les sources de contamination potentielles et de garantir l'origine des produits. Selon Walmart, l'utilisation de la chaîne de blocs a réduit le temps nécessaire pour suivre les produits contaminés de quelques jours à quelques secondes, ce qui a permis des rappels plus précis et plus rapides pour préserver la confiance des consommateurs dans l'industrie alimentaire (Higgins, 2017c). Walmart a fait un essai analogue pour les mangues.



Source : Provenance.

Les résultats encourageants des essais de Walmart sur la viande de porc et les mangues ont amené d'autres grandes entreprises alimentaires, comme Unilever, Nestlé et Kroger, à s'associer à IBM pour examiner comment la technologie de la chaîne de blocs pourrait être appliquée à leurs chaînes d'approvisionnement afin d'améliorer la traçabilité de leurs produits et de réduire le temps nécessaire pour identifier les sources de contamination (Hackett, 2017). En juin 2018, Walmart, Nestlé SA et huit autres sociétés ont formé un consortium utilisant la plate-forme de chaîne de blocs IBM Food Trust qui utilisera cette technologie pour suivre les produits alimentaires dans le monde entier (Giles, 2018). La plate-forme Food Trust reliera les producteurs, les transformateurs, les grossistes, les distributeurs, les fabricants, les détaillants et d'autres acteurs au moyen d'un registre avec permission afin d'accroître la visibilité et la responsabilité tout au long de la chaîne d'approvisionnement et de fournir aux participants des données sur l'origine des produits, sur la transformation et sur l'expédition, entre autres éléments. La traçabilité au moyen de la chaîne de blocs est, en fait, déjà une réalité. Walmart l'utilise au quotidien pour suivre plus de 25 lignes de produits, allant des produits laitiers aux aliments transformés et à la viande. En août 2018, Walmart avait suivi plus de 4 millions de lots de produits alimentaires sur une période d'environ 1 an.⁵

En mars 2017, la société chinoise de commerce électronique Alibaba a annoncé qu'elle s'associait à PricewaterhouseCoopers pour aider à résoudre les problèmes de sécurité sanitaire des produits alimentaires en Chine (Millward, 2017). Alibaba teste des utilisations de la chaîne de blocs pour suivre les produits alimentaires tout au long de la chaîne d'approvisionnement.

Dans certaines chaînes de valeur, la traçabilité peut être une exigence sanitaire, par exemple pour faire en sorte que les produits alimentaires soient exempts de maladies, comme l'encéphalopathie spongiforme bovine. L'application de tels systèmes de traçabilité est coûteuse, en particulier pour les pays en développement qui ont beaucoup de petites exploitations agricoles. La chaîne de blocs pourrait offrir une alternative intéressante aux systèmes complexes existants et faciliter l'accès aux marchés pour les exportateurs des pays en développement.

Au-delà des questions de qualité, la technologie de la chaîne de blocs est aussi utilisée par les entreprises pour vérifier les allégations éthiques et les pratiques commerciales équitables. En 2016, Provenance a piloté un projet en Indonésie, premier producteur mondial de thon, pour apporter la preuve que les produits sont issus de sources durables et exempts de toute forme d'esclavage.⁶ Les pêcheurs locaux envoyaient des SMS pour enregistrer leur prise dans la chaîne de blocs. L'identification était transmise à un fournisseur et chaque transaction qui avait lieu dans la chaîne d'approvisionnement était enregistrée. Les renseignements sur l'origine du produit et le parcours dans la chaîne d'approvisionnement pouvaient être

consultés et vérifiés par les acheteurs et les consommateurs finals au moyen de leurs smartphones. Ce projet pilote a montré comment la chaîne de blocs peut être utilisée pour suivre les poissons pêchés de manière responsable, vérifier les allégations sociales et rendre les chaînes d'approvisionnement du poisson plus transparentes. Un autre projet de Provenance a suivi le parcours des noix de coco de l'Asie du Sud-Est à l'Europe, afin de fournir aux acheteurs une preuve vérifiée par la chaîne de blocs de la juste rémunération des producteurs.⁷ La traçabilité des produits via la chaîne de blocs pourrait offrir de nouvelles possibilités aux producteurs des pays en développement, qui pourraient prouver plus facilement la qualité de leurs produits et négocier des prix justes.

La traçabilité des produits le long de la chaîne d'approvisionnement pour vérifier l'origine, la qualité et les allégations éthiques et sociales, et repérer les produits contaminés est indéniablement l'une des utilisations les plus prometteuses de la technologie de la chaîne de blocs. Dans une citation largement diffusée, Franck Yiannas, vice-président de Food Safety pour Walmart, a dit que la chaîne de blocs était « l'équivalent de [l'outil de suivi] FedEx Tracking pour les produits alimentaires » (Giles, 2018).

Toutefois, si l'utilisation de la chaîne de blocs peut améliorer la transparence et faciliter le suivi des produits le long de la chaîne d'approvisionnement, la chaîne de blocs garantit seulement que les informations qu'elle contient n'ont pas été falsifiées. Les tierces parties peuvent encore avoir à vérifier les processus hors chaîne et à confirmer qu'ils sont conformes aux allégations formulées. Les allégations éthiques et sociales via une chaîne de blocs, par exemple, valent ce que valent les processus de vérification hors ligne qui garantissent que les exigences éthiques et sociales ont été respectées hors chaîne. Il est donc essentiel d'établir un lien crédible entre les événements hors ligne et leur enregistrement en ligne. Dans l'une des premières études sur l'impact économique de la chaîne de blocs, Catalini et Gans (2017) notent que, s'il peut être assez simple et peu coûteux de vérifier les transactions portant sur des marchandises dont les attributs hors ligne sont faciles à appréhender et difficiles à altérer ou falsifier (par exemple les diamants), il est encore coûteux, dans bien des cas, de maintenir un lien robuste entre les événements hors ligne et les registres distribués et cela peut nécessiter non seulement un ou plusieurs intermédiaires fiables, mais souvent aussi plusieurs parties dans le même écosystème pour convenir de règles afin d'assurer la saisie et le partage sûrs des données. Connecter des produits physiques et des événements à une chaîne de blocs nécessite souvent des technologies sous-jacentes, comme l'Internet des objets. Cette connexion peut aussi constituer une vulnérabilité, car les produits physiques et les capteurs de l'Internet des objets peuvent être falsifiés (Carson *et al.*, 2018).

(b) Réduction des coûts du commerce

Dans leur étude de l'impact économique de la chaîne de blocs, Catalini et Gans (2017) identifient deux coûts essentiels influencés par la technologie : les coûts de vérification (c'est-à-dire la capacité de vérifier à peu de frais les attributs d'une transaction) et les coûts de mise en réseau (c'est-à-dire la capacité de lancer et d'exploiter un marché sans passer par un intermédiaire traditionnel).

Les exemples présentés dans le chapitre précédent confirment l'impact potentiellement important que la chaîne de blocs peut avoir sur les coûts de vérification, qui pourraient être réduits à presque rien du fait du caractère transparent et immuable de la technologie, conjugué à la possibilité d'automatiser les processus au moyen de contrats intelligents^{*}. Les renseignements ajoutés à la chaîne de blocs peuvent être automatiquement filtrés sur la base des conditions définies dans un contrat intelligent (par exemple pour traiter les demandes et les documents dans le cadre des procédures douanières ou les appels d'offres pour les marchés publics); les renseignements peuvent être facilement suivis et contrôlés; et le caractère immuable de la technologie facilite la vérification de l'identité des personnes et des registres financiers des entreprises.

Quant à l'impact de la technologie de la chaîne de blocs sur les coûts de mise en réseau, il est fort bien attesté par l'émergence de places de marchés pair à pair tels que OpenBazaar ou Hijro, dont le modèle économique consiste à profiter des possibilités offertes par la chaîne de blocs pour supprimer les intermédiaires traditionnels et réduire ainsi les coûts.

Le chapitre précédent montre également que la technologie pourrait avoir un impact beaucoup plus large sur les coûts. Étant donné qu'elle est décentralisée, très sûre et immuable et qu'elle permet d'automatiser les processus et les paiements, la chaîne de blocs pourrait réduire divers autres coûts du commerce, en particulier les coûts de traitement, de coordination, de transport, de logistique, d'intermédiation financière et de change. Son caractère décentralisé permet à de multiples entités de coordonner les actions en temps réel de manière transparente et sécurisée, ce qui accroît l'efficacité.

Le déploiement de la technologie de la chaîne de blocs pourrait avoir un effet considérable sur les coûts du commerce, mais celui-ci est difficile à évaluer. Comme on l'a vu dans la section 3.1 b), l'utilisation de la technologie de la chaîne de blocs pourrait aider à mettre en œuvre l'AFE de l'OMC, qui vise à faciliter les procédures douanières. L'OMC a estimé que la réduction moyenne des coûts du commerce pour toutes les exportations de marchandise qui résultera de la pleine mise en œuvre de l'AFE pourrait être de l'ordre de 14,3%, avec une réduction moyenne de

18% pour les produits manufacturés et de 10,4% pour les produits agricoles (OMC, 2015c).

L'examen de certaines estimations concernant le secteur financier et le secteur du transport maritime peut donner une idée plus précise de l'effet potentiel de cette technologie sur les coûts du commerce.

Dans une étude récente, Accenture et le spécialiste de benchmarking opérationnel McLagan estiment que le déploiement de la technologie de la chaîne de blocs dans les banques d'investissement pourrait permettre de réduire les coûts de 30% en établissant des processus plus efficaces et en améliorant la transparence et la mise en conformité (Accenture, 2017). De même, l'utilisation de la technologie de la chaîne de blocs pour les processus liés au commerce, y compris les procédures d'importation et d'exportation et les processus d'obtention de licences et de certificats, pourrait générer des économies considérables, dont les avantages seraient répartis entre les organismes concernés – car il faudrait moins de temps et de ressources pour traiter les demandes – et les commerçants – qui gagneraient du temps et économiseraient de l'argent.

On peut s'attendre aussi à des économies considérables dans le secteur du transport maritime, qui transporte environ 90% des marchandises échangées au niveau international.⁸ IBM a calculé que le transport d'un conteneur d'avocats de Mombasa à Rotterdam coûte environ 2 000 dollars EU, dont 300 dollars EU pour les formalités administratives. Selon IBM, la numérisation du processus pourrait réduire d'environ 15% le coût du transport maritime international, et une numérisation totale pourrait faire économiser aux transporteurs maritimes environ 38 milliards de dollars EU par an (Allison, 2017b). Bien que la numérisation puisse être assurée par d'autres moyens que la chaîne de blocs, les caractéristiques particulières de cette technologie en font un outil particulièrement intéressant pour faire avancer les efforts en ce sens, comme le montrent les différents exemples mentionnés dans la section 3.1.

McKinsey & Company estime que la valeur stratégique à court terme de la chaîne de blocs réside, en fait, principalement dans la réduction des coûts plutôt que dans la création de modèles économiques transformateurs. Sur la base d'une quantification de l'incidence monétaire de plus de 90 cas d'utilisation, McKinsey & Company conclut qu'environ 70% de la valeur en jeu à court terme consiste en la réduction des coûts (Carson *et al.*, 2018).

Des recherches plus poussées sont nécessaires pour tester et quantifier l'effet potentiel de la chaîne de blocs sur les différents types de coûts qui concernent les transactions commerciales internationales. Il semble à première vue que cet effet

est important. Dans une étude récente menée en collaboration avec Bain & Company, le Forum économique mondial a estimé que la suppression des obstacles grâce à la chaîne de blocs pourrait générer plus de 1 000 milliards de dollars EU d'échanges supplémentaires au cours des dix prochaines années (WEF, 2018). Il faut cependant considérer attentivement les coûts induits par l'adoption et le maintien d'un système basé sur la chaîne de blocs. La création d'une plate-forme de chaîne de blocs est une démarche complexe qui nécessite des processus d'intégration compliqués. En fait, il se peut que la réduction des coûts résultant d'une chaîne de blocs soit liée non pas à la technologie elle-même, mais plutôt au travail d'intégration et de rationalisation nécessaire pour passer à un système de chaînes de blocs.

Les réductions des coûts du commerce que l'utilisation de la technologie de la chaîne de blocs pourrait permettre ouvrent des possibilités particulièrement intéressantes pour les micro, petites et moyennes entreprises (MPME) dont les coûts fixes sont plus élevés, en proportion, que ceux des grandes entreprises, en particulier s'il s'agit de petits producteurs de pays en développement.

(c) Possibilités pour les MPME et les petits producteurs des pays en développement

Les MPME sont des acteurs économiques clés. Elles représentent plus de 90% des entreprises dans le monde et deux tiers de l'emploi total dans les pays en développement comme dans les pays développés. Toutefois, leur participation au commerce international est faible, leurs exportations représentant 7,6% des ventes du secteur manufacturier dans les pays en développement, contre 14,1% de celles des grandes entreprises manufacturières. Les chiffres sont un peu plus élevés dans les pays développés, où les MPME représentent 34% des exportations en moyenne (OMC, 2016c).

Les enquêtes sur les entreprises réalisées par diverses organisations gouvernementales et internationales⁹ indiquent que divers facteurs expliquent la participation limitée des MPME au commerce mondial : les droits de douane élevés, les multiples mesures non tarifaires, le manque de transparence et la lourdeur des procédures douanières, les difficultés d'accès aux renseignements relatifs au commerce, l'accès difficile aux réseaux de distribution, le manque de compétences et de technologie, les coûts de logistique et d'infrastructure, et l'accès insuffisant au financement du commerce. Ces difficultés sont communes à toutes les MPME des pays développés et en développement, mais elles ont tendance à toucher davantage les petites entreprises et les petits producteurs de pays en développement.

Comme on l'a vu dans le chapitre 3, la technologie de la chaîne de blocs peut aider à surmonter plusieurs de ces difficultés et peut être un moyen puissant de faciliter la participation des MPME au commerce international.

Les MPME, par exemple, ont plus de difficultés que les grandes entreprises à accéder au financement du commerce. Plus de la moitié de leurs demandes de financement du commerce sont rejetées, contre 7% pour les entreprises multinationales (OMC, 2016b) et des études ont montré qu'environ 60% des entreprises dont les demandes sont rejetées ne peuvent pas effectuer des transactions (Banque asiatique de développement, 2017). Des données empiriques suggèrent que les banques sont réticentes à consacrer de l'argent et des efforts à la connaissance de la clientèle, en particulier pour des clients potentiels qui ont peu de chances de générer des bénéfices importants. La rentabilité souvent faible des transactions des MPME, combinée au manque de données, financières et autres – qui rend difficile l'évaluation de leur solvabilité au moyen des méthodes traditionnelles – amènent les banques à refuser de leur accorder des garanties de crédit (Banque asiatique de développement, 2017).

La chaîne de blocs pourrait aider les petites entreprises et les petits producteurs à accéder au financement à trois niveaux.

Premièrement, son caractère immuable pourrait faciliter le suivi des transactions et l'évaluation de la solvabilité des entreprises et des personnes physiques – obstacle majeur pour les MPME et les petits producteurs. Allant un peu plus loin, 6 entreprises et banques internationales et 4 start-up de technologie financière ont annoncé en décembre 2017 le lancement d'un projet utilisant la technologie pour recueillir des renseignements sur le prix, la qualité et la durabilité du processus de production du riz de 10 000 riziculteurs malawiens afin de les aider à accéder à un financement à des conditions préférentielles compte tenu des éléments étayés par la chaîne de blocs (CISL, 2017).

Deuxièmement, les MPME n'ont souvent pas les ressources ni les capacités nécessaires pour faire face à des procédures complexes. La facilitation des procédures via la chaîne de blocs pour remédier au manque de financement des MPME – et créer, bien sûr, de nouveaux flux de revenus pour les banques – était au centre d'une initiative lancée par plusieurs banques en 2017. La plate-forme We.trade, accessible depuis n'importe quel appareil connecté, vise à simplifier les processus de financement du commerce pour les entreprises participantes, en particulier les petites, notamment la gestion, le suivi et la conclusion des transactions commerciales nationales et internationales. La plate-forme a achevé ses premières opérations en direct en juillet 2018 (voir aussi la section 3.1 a) et Suberg, 2018). D'autres plates-formes de financement du commerce, comme celle qui a été lancée

récemment dans la région de la baie de Guangdong (Hong Kong, Chine) et de Macao (Chine) avec le soutien de la banque centrale de Chine, visent spécifiquement les MPME.

Troisièmement, en permettant aux entreprises et aux personnes dans le monde entier d'effectuer des transactions directement de pair à pair sans avoir à passer par des banques, la technologie de la chaîne de blocs donne aux petites entreprises et aux petits producteurs la possibilité de participer au commerce international sans avoir besoin d'obtenir un financement du commerce traditionnel. C'est le cas, par exemple, de la plate-forme FastTrackTrade¹⁰, qui tire parti de cette technologie pour établir un réseau numérique de MPME afin de faciliter les transactions commerciales entre acheteurs et vendeurs et de donner aux entreprises participantes un accès direct aux services de financement du commerce de diverses sociétés de technologie financière, contournant ainsi les banques. Un autre exemple est la plate-forme de financement de la chaîne d'approvisionnement lancée par IBM en coopération avec un laboratoire de recherche technologique du Kenya et Twiga Foods, une plate-forme logistique interentreprises qui aide les agriculteurs à distribuer des bananes, des tomates, des oignons et des pommes de terre à 2 600 points de vente à travers le Kenya et qui utilise des algorithmes d'apprentissage automatique et la technologie de la chaîne de blocs pour accorder des microcrédits aux petites entreprises via des téléphones mobiles. L'essai de la plate-forme avec 220 petits détaillants de produits alimentaires dans tout le pays pendant 8 semaines a révélé que les clients avaient augmenté leurs commandes d'environ 30%. La plate-forme devrait être déployée dans toute l'Afrique vers la fin de 2018 (Wass, 2018a). Les enthousiastes de la chaîne de blocs considèrent qu'elle donne la possibilité de promouvoir l'inclusion financière dans les pays où une grande partie de la population n'est pas bancarisée (Société financière internationale, 2017).

Comme on l'a vu dans la section 3.1, la chaîne de blocs pourrait améliorer l'efficacité des procédures d'exportation et aider à administrer plus efficacement les guichets uniques, en permettant à toutes les parties autorisées d'interagir en temps réel et de manière pleinement transparente et sûre; en réduisant le volume des communications entre les parties, puisque chaque transaction est horodatée* et enregistrée dans la chaîne de blocs de manière quasi immuable et est visible pour tous les intéressés; en améliorant la traçabilité des transactions, et en rendant possible l'automatisation de certains processus grâce aux contrats intelligents. Si elle est déployée de manière appropriée à un coût qui justifie les bénéfices, la chaîne de blocs pourrait contribuer à la mise en œuvre de l'AFE et faciliter la participation des MPME au commerce international. L'ICC estime que l'AFE pourrait entraîner une augmentation d'environ 80% des exportations des MPME dans certaines économies en développement (Chambre de commerce internationale, 2017b).

La chaîne de blocs pourrait faciliter l'interaction des MPME avec les autorités douanières, mais aussi avec les consommateurs et les entreprises le long de la chaîne d'approvisionnement, en réduisant les coûts de transaction, ce qui permettrait aux MPME d'accroître leurs exportations. Comme l'indique un récent rapport du Parlement européen, les MPME pourraient compter parmi les principaux bénéficiaires de cette technologie (Parlement européen, 2018).

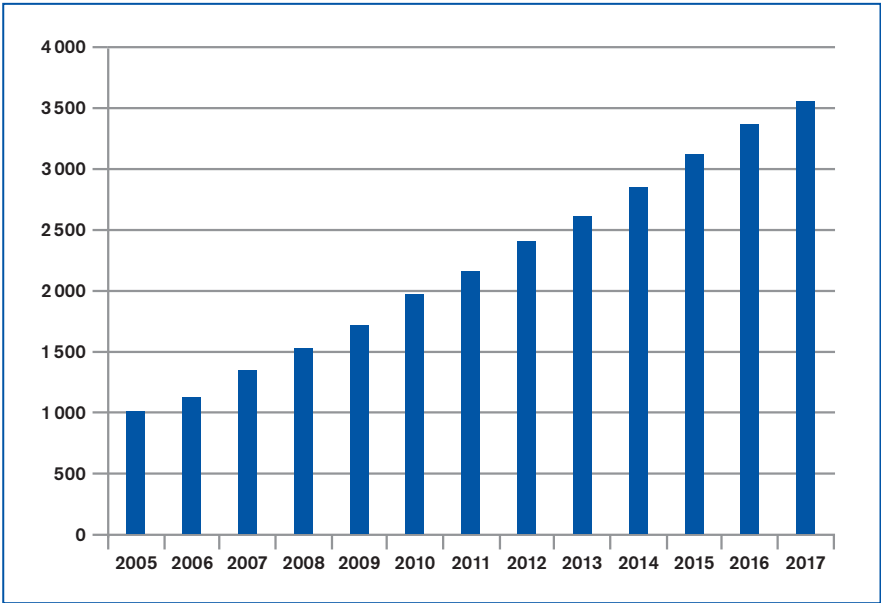
La chaîne de blocs permet de retracer plus facilement l'origine des produits (voir la section 4.1 a)), et cela peut aussi aider les petits producteurs des pays en développement à prouver la qualité de leurs produits et à négocier des prix justes. En août 2018, Oxfam a annoncé le lancement d'un projet pilote utilisant la technologie pour aider les riziculteurs cambodgiens à recevoir un meilleur prix pour leurs récoltes. Les petits agriculteurs manquent souvent de pouvoir et d'informations pour négocier les prix et les autres conditions avec les intermédiaires, les commerçants et les entreprises. L'application BlocRice vise à accroître la transparence et la traçabilité tout le long de la chaîne d'approvisionnement pour donner aux riziculteurs cambodgiens le pouvoir de négocier les prix et les aider à trouver des acheteurs.¹¹ Dans le même ordre d'idée, la chaîne de blocs pourrait aider les petits producteurs à défendre leur savoir traditionnel et leurs droits de propriété intellectuelle.

La passation des marchés publics en ligne est aussi largement préconisée comme un moyen efficace d'encourager la participation des MPME aux appels d'offres. La technologie de la chaîne de blocs pourrait améliorer l'efficacité des procédures d'appel d'offres et réduire les coûts pour que les petits fournisseurs puissent participer aux marchés publics.

En bref, la chaîne de blocs peut donner aux individus et aux entreprises du monde entier les moyens d'effectuer des transactions de manière plus efficace, économique et rapide. Elle pourrait réduire les obstacles à la participation au commerce international pour les petites entreprises et les petits producteurs, et elle pourrait favoriser grandement leur inclusion, à condition qu'ils aient les connaissances techniques nécessaires pour participer à la technologie – ou les ressources pour utiliser un fournisseur de service – et qu'ils disposent d'un accès adéquat à Internet.

Bien que le nombre de personnes connectées à Internet ait beaucoup augmenté (voir la figure 14), il reste beaucoup à faire pour combler le fossé numérique entre les économies avancées et les économies moins développées. Il subsiste des disparités importantes en termes d'accès et de bande passante. Près de 80% des Européens utilisent Internet, contre moins de 20% des Africains (voir la figure 15), et le fossé numérique entre les pays de l'Organisation de coopération et de développement économiques (OCDE) et les pays les moins avancés (PMA) s'est

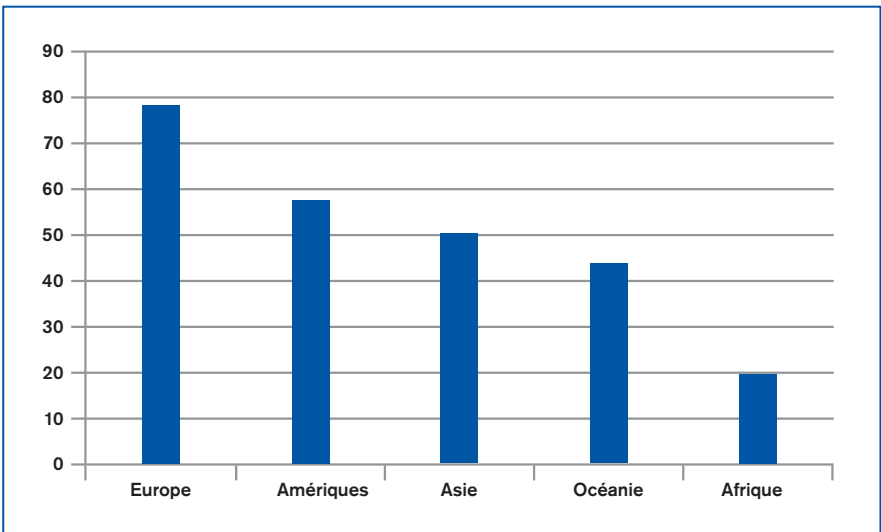
Figure 14 Nombre d'internautes, en millions, 2005-2017^a



Source : UIT/indicateurs des TIC.

^a Estimations.

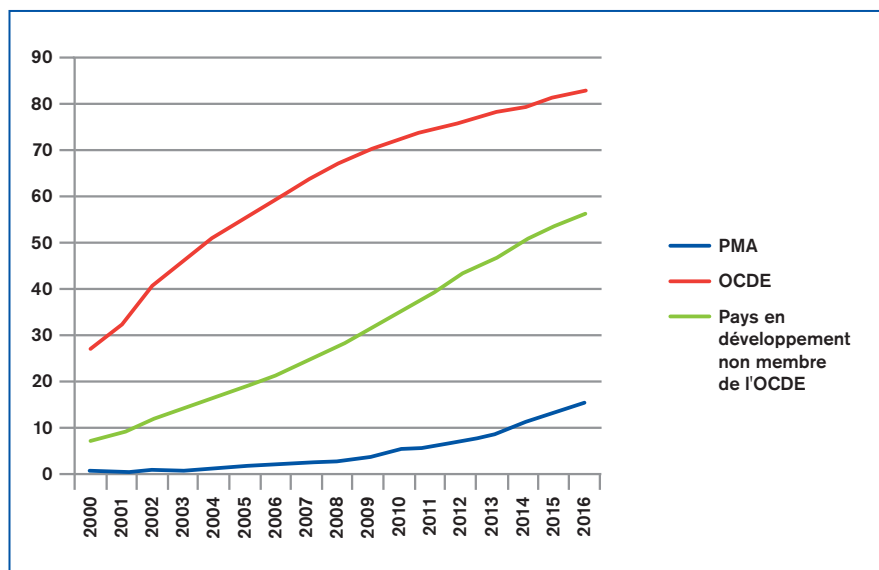
Figure 15 Proportion d'internautes (en pourcentage de la population) en 2015



Source : Calcul de l'auteure sur la base des indicateurs des TIC de l'UIT.

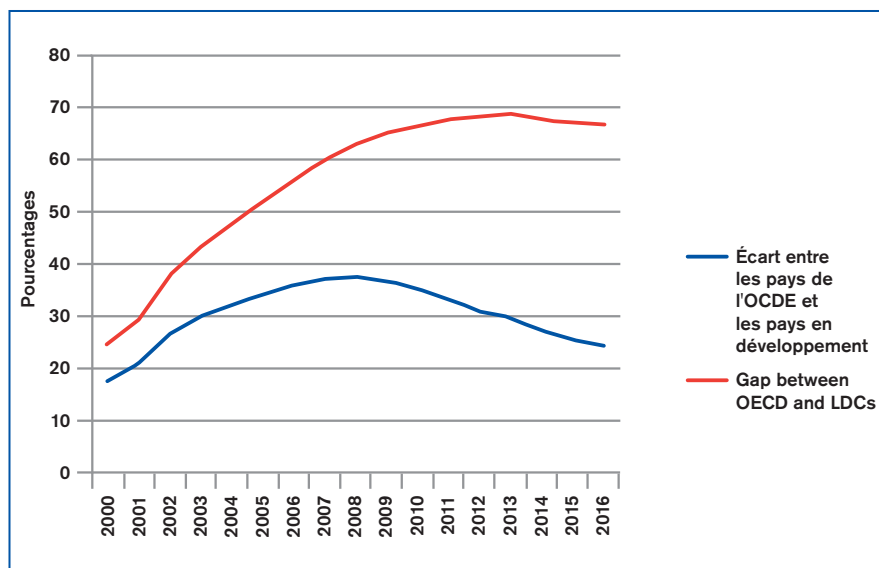
fortement creusé depuis le début du millénaire, malgré une légère amélioration depuis 2013 (voir les figures 16 et 17). Il y a encore beaucoup de chemin à parcourir pour atteindre l'Objectif de développement durable 9c des Nations Unies, qui

Figure 16 Proportion d'internautes (pour 100 habitants)



Source: Calculs de l'auteure sur la base des indicateurs des TIC de l'UIT.

Figure 17 Écart dans l'utilisation d'Internet (pour 100 habitants)

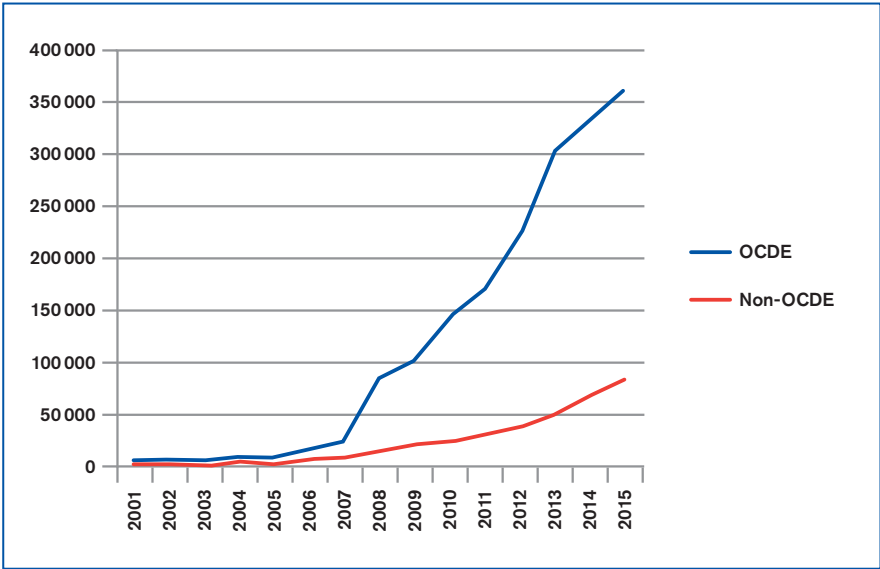


Source: Calculs de l'auteure sur la base des indicateurs des TIC de l'UIT.

demande à la communauté internationale d'«accroître nettement l'accès aux technologies de l'information et des communications et [de] faire en sorte que tous les habitants des pays les moins avancés aient accès à Internet à un coût abordable d'ici à 2020».¹²

L'écart croissant en termes de bande passante est plus préoccupant (voir la figure 18). Non seulement moins de personnes dans les pays en développement, en particulier les PMA, ont accès à Internet, mais encore elles ont accès à des installations de télécommunication moins puissantes et à un débit de bande passante limité. Les disparités mondiales en termes de distribution de la bande passante installée pour les télécommunications sont importantes et significatives : en 2014, trois pays seulement (la Chine, le Japon et les États-Unis) hébergeaient 50% du potentiel de bande passante installée dans le monde (Hilbert, 2016). Cette concentration n'est pas nouvelle – historiquement, dix pays détenaient de 70 à 75% de la capacité mondiale de télécommunication – mais si rien n'est fait dans les années à venir pour combler ce «double fossé», en termes d'accès à Internet et de capacité de bande passante, les inégalités continueront à croître, et le déploiement de technologies comme la chaîne de blocs pourrait accentuer les disparités en excluant de fait ceux qui n'ont pas la capacité technique d'y participer. Au lieu de profiter des possibilités qu'offre la technologie, les petites entreprises et les petits producteurs, en particulier ceux des pays en développement et des PMA, seront de

Figure 18 Bande passante internationale pour Internet par internaute (en bit/seconde)



Source: Calculs de l'auteure sur la base des indicateurs des TIC de l'UIT.

plus en plus laissés pour compte. Le risque n'est pas négligeable. Les faits montrent déjà que les MPME sont en retard dans l'adoption des technologies numériques (Organisation de coopération et de développement économiques, 2017).

Si la chaîne de blocs peut réduire les obstacles à l'entrée et faciliter la participation des MPME et des petits producteurs au commerce international, il se peut que certains secteurs en bénéficient plus que d'autres. L'émergence de nouveaux modèles économiques basés sur des plates-formes de chaînes de blocs ou articulés autour d'elles pourrait bouleverser des secteurs entiers, obligeant les entreprises existantes, notamment les petites entreprises, à s'adapter pour ne pas être laissées pour compte. La crainte de céder du terrain face aux concurrents peut expliquer le nombre d'entreprises, en particulier dans le secteur des services – services financiers, services d'assurance, de logistique, de distribution, etc. – qui s'empressent d'examiner le potentiel de la chaîne de blocs.

Toutefois, il est probable que les obstacles à l'entrée ne disparaîtront pas pour tout le monde. Les simples utilisateurs des plates-formes de chaînes de blocs ont des chances de bénéficier de la réduction des obstacles, mais les entreprises qui sont en concurrence directe avec les « initiés de la plate-forme », c'est-à-dire avec les entreprises qui sont les « gardiens » d'une plate-forme avec permission (telles que les banques participantes dans le cas d'une plate-forme gérée par des banques), se heurteront probablement à des obstacles plus importants. Le niveau d'investissement nécessaire pour devenir l'un des gardiens d'une plate-forme avec permission pourrait exclure les retardataires et rendre plus difficile pour les nouveaux venus de se développer sur un marché donné. Si les MPME ont des chances d'être bénéficiaires en tant qu'utilisatrices, elles pourraient avoir plus de difficultés à devenir des « initiées de la plate-forme ». Certains observateurs notent que, si la chaîne de blocs peut accroître la concurrence en facilitant l'entrée, elle peut aussi conduire à plus de collusion, et il ne peut pas être exclu qu'une seule chaîne de blocs devienne dominante en raison des effets de réseau, ce qui aboutirait à une réduction de la concurrence et à des obstacles plus importants à l'entrée, dont les MPME pourraient pâtir de manière disproportionnée (Cong, 2018).

La technologie peut faciliter la participation des MPME et des petits producteurs au commerce international mais, comme toute innovation, elle porte aussi en elle le risque de perturber certains secteurs et certaines catégories de travailleurs. Il se peut que les possibilités et les avantages ne soient pas également répartis.

2. Le succès n'est pas acquis

La chaîne de blocs ouvre des perspectives intéressantes en termes de réduction des coûts, d'efficacité, de traçabilité et de sécurité, mais il y a un certain nombre de défis à surmonter avant que la technologie puisse être utilisée à grande échelle.

(a) Défis technologiques

(i) Le défi de la scalabilité : la chaîne de blocs peut-elle être déployée à grande échelle ?

Alors que certains observateurs pensent que la technologie de la chaîne de blocs peut modifier radicalement la façon dont nos sociétés fonctionnent (Boucher, 2017), beaucoup soulignent aussi que la scalabilité des chaînes de blocs est limitée en raison de la taille prédéterminée des blocs et des problèmes de consommation d'énergie. Cela est particulièrement vrai pour les chaînes de blocs publiques, mais moins pour les chaînes de blocs de consortium et privées, qui ne connaissent pas les mêmes limitations.

La scalabilité est probablement l'un des plus grands défis rencontrés dans le cas des chaînes de blocs publiques. Elle fait l'objet de débats intenses dans la communauté de la chaîne de blocs. Par exemple, alors que Bitcoin a une limite théorique de 4 000 transactions par seconde, le réseau traite environ 7 transactions par seconde en moyenne¹³ et Ethereum environ deux fois plus.¹⁴ À titre de comparaison, les prestataires de services de paiement traditionnels comme Visa peuvent traiter 2 000 transactions par seconde en moyenne avec un maximum de 56 000 transactions par seconde (Croman *et al.*, 2016). Comme le nombre de transactions de chaînes de blocs augmente de façon exponentielle – les transactions quotidiennes sur le réseau Ethereum, par exemple, ont augmenté de 500% entre le début de 2016 et le début de 2017 (Croman *et al.*, 2016) – les chaînes de blocs publiques sont de plus en plus congestionnées, ce qui entraîne des retards supplémentaires dans la validation des transactions.

L'augmentation rapide du nombre de transactions a conduit la communauté des cryptomonnaies à réfléchir à des solutions possibles pour résoudre le problème de la scalabilité. Il a récemment été décidé de doubler la taille des blocs sur Bitcoin de 1 Mo à 2 Mo, et d'appliquer une nouvelle technologie – appelée « segregated witness » (SegWit) – pour réduire la quantité de données à vérifier dans chaque bloc afin d'accélérer la validation des blocs (Marshall, 2017). Parmi les autres solutions proposées applicables à d'autres chaînes comme Ethereum, il y a, par exemple, la

possibilité d'effectuer certaines interactions hors de la chaîne de blocs (par la création de «canaux d'état»), de partitionner les données de la chaîne de blocs en «shards»* (c'est-à-dire en plusieurs segments de réseau) et de faire des calculs hors chaîne.¹⁵ D'autres projets proposent un compromis en limitant le nombre de nœuds* nécessaires pour valider une transaction au prix d'une certaine centralisation. Cependant, aucune de ces solutions ne peut à elle seule résoudre le problème de la scalabilité des chaînes de blocs publiques, et une combinaison d'approches sera probablement nécessaire.

Toutefois, il est important de noter que les chaînes de blocs de consortium avec permission, lesquelles sont largement utilisées dans des applications liées au commerce international, ne sont pas soumises aux mêmes limitations. Elles peuvent utiliser des protocoles nécessitant moins de puissance de calcul pour vérifier les transactions et elles sont donc plus facilement scalables. Par exemple, Hyperledger Fabric, qui est un système d'exploitation distribué pour les chaînes de blocs avec permission, peut traiter 3 500 transactions par seconde pour certains plans de charge (Androulaki *et al.*, 2018). Étant donné que les chaînes de blocs avec permission contrôlent chaque nœud dans le réseau, elles peuvent faire en sorte que chaque nœud soit un ordinateur avec un accès Internet haut débit et une grande puissance de calcul, laquelle est augmentée quand cela est nécessaire pour que le réseau ne soit pas congestionné. Il est toutefois essentiel que les organismes ou les entreprises qui se tournent vers la chaîne de blocs gardent à l'esprit ces besoins de scalabilité pour faire en sorte que leurs systèmes de chaîne de blocs conservent leur efficacité et leur pertinence initiales au fil du temps.

Enfin, il convient de noter que les problèmes de scalabilité concernent certaines technologies de registres distribués plus que d'autres. La grande majorité des nouveaux articles et études sont axés sur la chaîne de blocs du bitcoin. Mais d'autres technologies de registres distribués qui ne traitent pas les transactions en blocs peuvent traiter un nombre beaucoup plus élevé de transactions (voir le tableau 2). La technologie est encore en train d'évoluer et de nouvelles variantes permettant une plus grande scalabilité sont mises au point. HashGraph, par exemple, lancé en 2017, utilise un nouvel algorithme de consensus* qui pourrait lui permettre de traiter les transactions 50 000 fois plus vite que Bitcoin, la seule limite étant la bande passante – c'est-à-dire plus de 250 000 transactions par seconde –, ce qui amène certains observateurs à dire que la chaîne de blocs est déjà obsolète et qu'HashGraph représente l'avenir des registres distribués.¹⁶ Il reste cependant à voir si HashGraph ou une autre variante de la DLT parviennent à traiter rapidement un grand nombre de transactions à grande échelle.

Tableau 2 Commission et durée de transaction moyennes, capacité de transaction et efficacité énergétique pour les dix principales cryptomonnaies

Cryptomonnaie	Commission de transaction moyenne en dollars EU	Durée de transaction moyenne	Capacité de transaction par seconde	Efficacité énergétique	Caractéristiques supplémentaires
1. Bitcoin	7,32	9-10 minutes	7	Faible (chaîne de blocs PoW)	
2. Ethereum	0,22	14 secondes	20	Faible (chaîne de blocs PoW)	Supporte les contrats intelligents
3. Bitcoin Cash	0,32	9-10 minutes	50	Faible (chaîne de blocs PoW)	
4. Ripple	0,0000024 (+ commission IOU)	3,5 secondes	1 000	Élevée (algorithme de vote)	Permet les transactions IOU dans n'importe quelle monnaie
5. Litecoin	0,15	2 minutes	56	Faible (chaîne de blocs PoW)	
6. Dash	0,30	2-3 minutes	(4 000)	Faible (chaîne de blocs PoW)	
7. NEO	Aucune (+commission variable)	Quelques secondes	1 000	Élevée (algorithme de vote)	Supporte les contrats intelligents
8. IOTA	Aucune	Aucunes données disponibles	500-800	Assez élevé (Tangle PoW)	Particulièrement adapté aux dispositifs IdO
9. Monero	2,43	2 minutes	1 700	Faible (chaîne de blocs PoW)	Caractéristiques de confidentialité avancées
10. NEM	0,21	30 secondes	(3 000)	Élevée (chaîne de blocs Pol)	Système de réputation intégré

Il convient de noter que ce tableau repose sur des données datant du 20 novembre 2017. Il donne un aperçu de la situation et peut changer considérablement en peu de temps. En outre, la précision des données sur les durées et les capacités de transaction varie et les données reposent parfois uniquement sur des estimations. Le tableau devrait toutefois permettre au lecteur de se faire une idée approximative des vitesses et des capacités des cryptomonnaies mentionnées. [PoW = preuve de travail ; Pol = preuve d'importance]

Source: Ohnesorge (2018).

(ii) Le débat sur l'énergie : surtout un problème pour les chaînes « sans permission »

L'une des plus vives controverses autour de la chaîne de blocs a trait à sa consommation d'énergie. Comme les préoccupations environnementales sont au premier plan dans l'agenda international, certains observateurs notent que l'utilisation accrue de la DLT pourrait aller à l'encontre de l'objectif de réduction des émissions de carbone.

En effet, le processus de validation des blocs peut nécessiter, dans certaines chaînes de blocs, une grande puissance de calcul et une grande quantité d'énergie – ce qui a une incidence directe sur le potentiel de scalabilité de la chaîne de blocs correspondante. Cela est particulièrement vrai pour les transactions Bitcoin. O'Dwyer et Malone (2014) montrent qu'en 2014, la chaîne de blocs Bitcoin a consommé à peu près autant d'électricité que l'Irlande, soit environ 3 GW.

Ces chiffres posent clairement la question de la durabilité, d'autant que le déploiement de la technologie est encore limité. S'il est légitime de suivre de près l'évolution de l'empreinte énergétique des plates-formes de chaînes de blocs, on ne peut pas généraliser sur la base des chiffres mentionnés ci-dessus. En effet, les plates-formes de chaînes de blocs reposent sur différents types d'algorithmes qui consomment plus ou moins d'énergie (voir le tableau 2). Bitcoin, par exemple, est beaucoup plus énergivore que la chaîne de blocs publique Ethereum – 163 kilowatts/heure (KWh) par transaction contre 49 KWh (Coppock, 2017). En fait, le débat sur l'énergie découle principalement de la forte consommation de la chaîne de blocs Bitcoin. Or les chaînes de blocs avec permission utilisent des mécanismes de consensus beaucoup plus légers, qui consomment beaucoup moins d'énergie. Par ailleurs, des algorithmes plus économes en énergie sont mis au point, tels qu'IOTA ou, plus récemment HashGraph, un nouveau type de registres distribués qui serait 50 000 fois plus rapide que Bitcoin et qui réduit considérablement la puissance de calcul et la quantité d'énergie requises pour valider les transactions.

Les promoteurs de la chaîne de blocs notent en outre que, au-delà du bitcoin, cette technologie peut aider à accroître l'efficacité énergétique. L'utilisation de contrats intelligents pourrait permettre aux entreprises de services publics d'exploiter leur réseau plus efficacement grâce à un meilleur équilibre entre l'offre et la demande en temps réel (T'Serclaes, 2017). Sur cette base, le déploiement de la technologie de la chaîne de blocs pourrait remanier les modèles de services publics et de consommation et conduire à une plus grande efficacité énergétique.

Les nouvelles technologies et les nouveaux processus, une fois mis au point, ne sont pas gravés dans le marbre. Leurs caractéristiques et leur usage varient dans le temps. Ceux qui réussissent sont ceux qui s'adaptent aux contraintes du moment et qui deviennent ainsi durables. Cela vaut aussi pour la technologie de la chaîne de blocs : c'est seulement si l'on réussit à élaborer des algorithmes plus économes en énergie que l'on pourra envisager son adoption à grande échelle.

(iii) Sécurité : est-ce sûr et pour combien de temps ?

Bien que les chaînes de blocs soient très résistantes par rapport aux bases de données traditionnelles en raison de leur caractère décentralisé et distribué et de l'utilisation de techniques cryptographiques, elles ne sont pas complètement à l'abri des problèmes de sécurité traditionnels. Le fait que les données sont distribuées entre les nœuds participants facilite grandement la récupération après un sinistre : si un nœud est compromis, les données de la chaîne de blocs peuvent être récupérées à partir des autres nœuds participants. L'absence de point de défaillance unique (et donc d'entité centrale à pirater) fait qu'il est difficile de compromettre l'ensemble du réseau. Toutefois, une attaque à 51%, dans laquelle la majorité des nœuds sont compromis, reste possible en théorie, en particulier dans le cas des chaînes de blocs avec permission, qui comptent beaucoup moins de nœuds que les chaînes de blocs publiques – bien qu'une telle attaque soit assez difficile dans la pratique. Le lancement par Vitalik Buterin d'un nouvel algorithme de consensus en août 2018, qui obligerait un attaquant qui souhaite contrôler le réseau à contrôler 99% des nœuds de la chaîne de blocs au lieu de 51% seulement, pourrait changer la donne (Buterin, 2018) et rendre les attaques encore plus difficiles. La plus grande vulnérabilité vient, en fait, des contrats intelligents, comme l'a montré l'attaque de DAO* de 2016, et des interfaces utilisateurs (mobiles, ordinateurs portables, etc.).

Un autre point important à garder à l'esprit est que la résistance de la chaîne de blocs repose sur le chiffrement* et les algorithmes, dont la solidité dépend de la puissance de calcul. Les progrès de la technologie, en particulier l'informatique quantique, pourraient, à terme, représenter une menace pour la technologie de la chaîne de blocs. Pour l'heure, les ordinateurs quantiques expérimentaux n'ont pas une puissance de calcul suffisante pour casser les algorithmes cryptographiques. Toutefois, la communauté des cryptographes se prépare. Les algorithmes post-quantiques, susceptibles de résister à l'informatique quantique, font l'objet de recherches intenses.

Ces défis sont considérables, mais la technologie est encore en train d'évoluer et des solutions technologiques sont étudiées et mises au point.

(b) Défis de l'interopérabilité

L'avènement de la chaîne de blocs pose des problèmes d'interopérabilité tant au niveau technique (comment les différentes interfaces techniques communiquent entre elles) qu'au niveau sémantique (comment l'information échangée est-elle comprise par les diverses parties concernées). Ces défis ne sont pas propres à la chaîne de blocs mais, comme pour les autres technologies numériques, s'ils ne sont pas résolus, bon nombre des avantages potentiels de la chaîne de blocs seront remis en cause.

(i) *Le problème des îlots numériques*

Un défi important est celui de l'interopérabilité des différentes chaînes de blocs existantes, problème rendu plus aigu par la recherche d'alternatives pour développer des applications qui répondent aux besoins spécifiques des différentes branches d'activité et qui suivent souvent des approches algorithmiques différentes. De nombreuses plates-formes en cours de construction ne « communiquent pas entre elles ». Par exemple, les projets pilotes d'IBM utilisent Hyperledger Fabric, alors que l'offre de chaîne de blocs de Microsoft repose sur la chaîne de blocs Ethereum. Par ailleurs, le consortium R3CEV a mis au point sa propre plate-forme DLT, Corda. La start-up Provenance utilise la chaîne de blocs Ethereum, alors que d'autres entreprises qui proposent des solutions basées sur la chaîne de blocs pour suivre les produits et accroître la transparence de la chaîne d'approvisionnement, comme Everledger, reposent sur Hyperledger Fabric. Bien que chacun de ces projets soit intéressant individuellement, le manque d'interopérabilité des plates-formes sur lesquelles ils ont été construits limite l'utilisation et la scalabilité de la technologie et des projets. Il est certes possible d'établir des passerelles *ad hoc* entre deux plates-formes données, mais il n'est pas facile d'augmenter l'échelle de telles solutions faites sur mesure.

Les questions d'interopérabilité revêtent une importance particulière pour le commerce international, car un seul envoi commercial international peut concerner plusieurs registres, de la finance à la logistique, aux douanes et à la provenance.

Le développement de solutions d'interopérabilité¹⁷ est donc essentiel pour éviter les conflits entre des approches disparates et pour faire en sorte que les réseaux de chaînes de blocs communiquent entre eux, ce qui permettrait d'exploiter pleinement le potentiel de la technologie. La communauté de la chaîne de blocs est bien consciente des enjeux et elle recherche activement des solutions techniques.

Alors que l'idée d'une interaction entre différentes chaînes de blocs semblait encore une lointaine possibilité il y a à peine un an ou deux, des solutions concrètes

commencent maintenant à voir le jour. Au niveau intra-registres, l'Enterprise Ethereum Alliance, par exemple, a dévoilé, en mai 2018, un cadre multiplates-formes libres fondé sur des normes pour les chaînes de blocs avec permission basées sur Ethereum qui permettrait l'interopérabilité des chaînes de blocs avec permission construites sur la chaîne de blocs publique Ethereum (Higgins, 2018).

Pour important qu'il soit, ce fait nouveau ne résoudra pas le problème de l'interopérabilité des registres reposant sur différentes plates-formes, mais à cet égard aussi, les choses avancent. Des travaux sont en cours dans le cadre du projet Hyperledger pour développer diverses solutions d'interopérabilité inter-registres, tels que Hyperledger Sawtooth et Hyperledger Burrow, qui peuvent exécuter le code des contrats intelligents d'Ethereum¹⁸, et Hyperledger Quilt, qui propose l'interopérabilité entre systèmes de registres en appliquant un protocole de paiements pour transférer la valeur entre les systèmes.¹⁹ Également en mai 2018, deux start-up, Clearmatics et Axoni, ont démontré comment un produit financier dérivé pouvait être créé dans la chaîne de blocs d'une entreprise et implanté dans une autre. L'interopérabilité apparaît à présent comme un objectif de conception essentiel de la technologie des registres distribués (Allison, 2017a).

En outre, en novembre 2017, les entreprises à l'origine de trois plates-formes de chaînes de blocs – Aion, ICON et Wanchain – ont annoncé la création d'un nouveau groupe de plaidoyer, la Blockchain Interoperability Alliance, qui vise à élaborer des normes mondialement acceptées pour promouvoir une plus grande connectivité et interopérabilité entre les différents réseaux de chaîne de blocs (Higgins, 2017a). Joe Lubin, co-fondateur d'Ethereum, Adam Back, scientifique pour Bitcoin, Brian Behlendorf, directeur exécutif d'Hyperledger, et Richard Gendal Brown, du consortium de registres distribués R3, étudient ensemble des approches permettant de rendre les réseaux interopérables, en développant des « inter-registres » capables de faciliter l'interopérabilité, ou une solution d'identité permettant aux utilisateurs de posséder leurs propres profils (Del Castillo, 2017).

La multiplicité des plates-formes a aussi des conséquences plus concrètes, en particulier en ce qui concerne le commerce international, car une expédition internationale peut concerner une douzaine de registres différents. Pour les parties intervenant dans ces transactions, l'hébergement d'une douzaine de nœuds serait trop difficile. La communauté de la chaîne de blocs est en train d'examiner une approche consistant à créer un système d'authentification inter-registres pour permettre aux parties autorisées de vérifier les transactions, quel que soit le registre sur lequel elles sont créées (CEFACT-ONU, 2018). L'authentification inter-registres pourrait être effectuée par une seule entité ou par différentes entités, mais moyennant la réintroduction d'un certain degré de centralisation.

(ii) Normalisation des données

Au-delà des aspects purement techniques de l'interopérabilité au niveau des interfaces, des difficultés tout aussi importantes existent pour aligner la sémantique (c'est-à-dire la signification des informations échangées), développer des ensembles de données types englobant toutes les données utilisées pour l'échange de renseignements concernant l'importation, l'exportation, le transit, le transport et le financement, et pour harmoniser les processus. Bien souvent, les douanes, les entreprises de logistique et les commerçants, par exemple, n'utilisent pas la même sémantique et voient les données différemment. Le «port de débarquement» correspond-il au «lieu de déchargement»? L'«identification du produit» correspond-elle au code de la nomenclature nationale (utilisé par les douanes), à l'expression «qui dit contenir» (utilisée par les entreprises de transport) ou au code de la classification globale des produits (utilisé par les commerçants)? Cette question a été examinée de près au cours des dernières années pour faire en sorte que les différentes parties concernées comprennent les mêmes données de la même manière. Le CEFAC-ONU et l'OMD ont tous deux travaillé sur des modèles de données afin d'élaborer un langage universel pour l'échange de données transfrontières. Le CEFAC-ONU, par exemple, propose sa bibliothèque de composants communs²⁰ et des modèles de données de référence connexes comme éléments constitutifs de base des chaînes de blocs pour améliorer l'interopérabilité des données et a élaboré une recommandation sur la simplification et la normalisation des données (recommandation n° 34), tandis que l'OMD a développé son propre modèle de données.²¹ Ces difficultés, qui sont liées à la numérisation du commerce, sont antérieures à l'avènement de la chaîne de blocs. Toutefois, le développement des cas d'utilisation de la chaîne de blocs couvrant les différentes étapes du commerce international, du financement du commerce jusqu'aux procédures douanières, en passant par le transport et la logistique, rend une approche multipartite sur ces questions encore plus indispensable.

D'autres organisations internationales se penchent sur les questions d'interopérabilité technique et sémantique. En juin 2017, la Commission bancaire de la Chambre de commerce internationale (ICC) a établi un groupe de travail composé de leaders des secteurs de la banque, de la technologie financière et des entreprises pour créer un ensemble de normes minimales auxquelles les sociétés de technologie financière peuvent adhérer afin de remédier au problème des «îlots numériques» (Chambre de commerce internationale 2017c). Des travaux sont également en cours à l'Union internationale des télécommunications (UIT) et à l'Organisation internationale de normalisation (ISO). Le Secteur de la normalisation des télécommunications de l'UIT a créé, en mai 2017, un groupe de réflexion sur l'application de la technologie des registres distribués. Le groupe établira, entre autres, une feuille de route de normalisation pour l'interopérabilité des services

basés sur la DLT, en tenant compte des activités en cours à l'IUT et dans d'autres organisations, forums et groupes chargés d'élaborer des normes.²² Quant à l'ISO, elle a créé un comité en 2016 (comité ISO/TC/307) pour établir des normes afin de « permettre une meilleure interopérabilité, une adhésion plus rapide et davantage d'innovation dans [l']usage et [l']application » de la technologie de la chaîne de blocs. Ce comité, qui comptait 35 pays participants et 13 observateurs en juillet 2018, a tenu sa réunion inaugurale à Sydney (Australie) en mai 2017. Plusieurs groupes de travail ont été mis sur pied pour examiner les questions concernant les cas d'utilisation, la gouvernance, l'interopérabilité, la sécurité, la confidentialité, l'identité et les contrats intelligents, et pour établir des normes (Naden, 2017). Dix normes ISO sont en cours d'élaboration.

Les enjeux sont considérables. En effet, le développement de systèmes incompatibles irait à l'encontre de l'objectif global de la technologie de la chaîne de blocs, qui est d'assurer une plus grande intégration des processus d'une manière transparente et dynamique, mais en plus, cela pourrait s'avérer contre-productif car cela cloisonnerait les processus dans des silos techniques, et le non alignement de la sémantique annulerait les avantages potentiels de la chaîne de blocs. Il est donc essentiel de résoudre les problèmes d'interopérabilité à la fois au niveau technique et sémantique et au niveau des données.

(c) Questions juridiques

Le déploiement à grande échelle de la chaîne de blocs exige plus que de la technologie. Il nécessite des cadres qui garantissent l'interopérabilité des réseaux, et qui clarifient aussi le statut juridique des transactions de la chaîne de blocs et réglementent les responsabilités et la façon dont les données peuvent être consultées et utilisées. Sans ce volet réglementaire, la technologie de la chaîne de blocs pourrait bien être cantonnée à des projets pilotes.

Les questions juridiques soulevées par l'utilisation de la chaîne de blocs sont de deux types : les questions générales, telles que le statut juridique des transactions de la chaîne de blocs et les questions de juridiction ; et les questions spécifiques liées à l'utilisation de la chaîne de blocs dans des cas particuliers. Pour certaines questions douanières, par exemple, une autorisation délivrée par une entité particulière peut être nécessaire pour automatiser certains processus au moyen de contrats intelligents. Ces questions particulières dépendent de la nature de l'application de la chaîne de blocs qui est élaborée ; elles ne sont pas abordées dans cette section, mais elles doivent être prises en compte par les autorités et les entreprises qui s'intéressent aux utilisations de la chaîne de blocs.

(i) Validité juridique des transactions de la chaîne de blocs

Le statut juridique des transactions de la chaîne de blocs et des contrats intelligents reste incertain, sans parler de celui des instruments financiers émis sur une chaîne de blocs.²³ Les transactions de la chaîne de blocs posent des questions de classification (Werbach, 2018). Comment classer des activités qui sont légitimes, mais qui ne sont pas structurées selon les exigences juridiques du monde extérieur à la chaîne de blocs ?²⁴ Les renseignements stockés sur une chaîne de blocs représentant la propriété ou l'existence d'un actif prouvent-ils la propriété réelle ou l'existence réelle de cet actif ? Dans quelle mesure un tribunal reconnaîtrait-il la chaîne de blocs comme une source de vérité immuable et infalsifiable (Cermeno, 2016) ? Les contrats intelligents sont-ils des contrats juridiques ? Les obligations et les instruments dérivés émis sur une chaîne de blocs ont-ils une validité juridique ?

Certaines initiatives ont été prises au niveau international pour tenter de clarifier le statut juridique de ces transactions et processus. Le 13 juillet 2017, la CNUDCI a adopté la Loi type sur les documents transférables électroniques, attendue de longue date (Service d'information des Nations Unies, 2017). La Loi type permet l'utilisation de documents transférables électroniques et énonce les conditions à remplir pour qu'un document électronique soit considéré comme un document transférable, c'est-à-dire un document qui donne le droit au titulaire de revendiquer l'exécution de l'obligation indiquée dans le document – comme dans le cas des connaissements, des lettres de change, des billets à ordre et des récépissés d'entrepôt. Le principe de neutralité inscrit dans la Loi type permet de tenir compte de l'utilisation de toutes les méthodes et technologies, y compris les registres distribués.

L'adoption de la Loi type de la CNUDCI sur les documents transférables électroniques est une avancée importante qui peut ouvrir la voie à l'utilisation légale de la technologie de la chaîne de blocs pour les transactions commerciales internationales si la loi est transposée dans la législation nationale. La Loi type complète utilement les principes de la CNUDCI qui guident le commerce électronique. Conformément au principe de neutralité technologique inscrit dans la Loi type sur le commerce électronique (1996, révisée en 1998), dans la Loi type sur les signatures électroniques (2001) et dans la Convention sur l'utilisation de communications électroniques dans les contrats internationaux (2005), un message de données stocké sur une chaîne de blocs est réputé satisfaire aux exigences applicables aux documents papiers concernant l'écriture et la signature, à condition qu'il remplisse les conditions correspondantes (Takahashi, 2017). Néanmoins, la Loi type ne porte pas sur les cryptomonnaies. Une législation distincte sera nécessaire pour définir les conditions dans lesquelles les jetons (tokens) basés sur la chaîne de blocs représentant des valeurs mobilières (cryptovaleurs) peuvent être traités comme telles.

Les lois types de la CNUDCI sont certes importantes en termes d'orientations législatives, mais elles n'ont aucune valeur juridique en soi. Ce sont uniquement des modèles qui peuvent servir de base à la législation des pays.

Plusieurs gouvernements sont en train d'élaborer des lois pour reconnaître la validité juridique des signatures sur la chaîne de blocs, des contrats intelligents et des instruments financiers émis sur la chaîne de blocs. En 2017, au moins huit états des États-Unis ont rédigé des projets de loi acceptant ou encourageant l'utilisation du bitcoin et de la technologie de la chaîne de blocs, et quelques-uns les ont déjà adoptés (Parker, 2017). Un projet de règlement légalisant les signatures sur la chaîne de blocs et les contrats intelligents a été adopté en Floride au début de 2018. On peut citer d'autres exemples, comme Malte – qui a adopté en juillet 2018 une loi réglementant la technologie des registres distribués et les actifs financiers virtuels dans le but de promouvoir Malte en tant qu'«île de la chaîne de blocs» (Alexandre, 2018), et comme la France, qui a pris plusieurs initiatives pour reconnaître les instruments financiers émis sur les chaînes de blocs. En 2016, la France a modifié sa législation pour reconnaître certaines mini-obligations émises sur les chaînes de blocs, et, en décembre 2017, elle a publié un décret permettant l'enregistrement et le transfert de valeurs financières via la technologie DLT.²⁵ Un autre fait nouveau intéressant est la décision de la Cour suprême chinoise de septembre 2018, selon laquelle les preuves authentifiées par la chaîne de blocs sont recevables dans les différends juridiques (Huillet, 2018b).

Plusieurs propositions concernant directement la chaîne de blocs ont aussi été présentées à l'OMC dans le cadre de la déclaration conjointe sur le commerce électronique. Elles portent sur des questions telles que l'authentification électronique, la reconnaissance des documents électroniques et des signatures électroniques, l'établissement d'un cadre pour les contrats électroniques, le chiffrement, la cybersécurité, les paiements électroniques et la protection des données personnelles.²⁶ Comme cela a été dit précédemment, si la chaîne de blocs peut contribuer à la numérisation du commerce, le passage au commerce sans papier nécessite un cadre réglementaire favorable qui reconnaît la validité des signatures électroniques, des documents électroniques et des transactions électroniques et qui fixe les paramètres juridiques de l'échange électronique de données entre les parties prenantes concernées, en particulier les autorités gouvernementales (voir la section 3.1 b)).

Certains observateurs notent cependant que, comme la technologie est encore en train d'évoluer, il est peut-être trop tôt pour la réglementer. Ils estiment qu'une réglementation précoce risquerait de freiner son développement et de limiter son potentiel, sans réglementer convenablement son utilisation (R3 et Norton Rose Fulbright, 2017 ; Orcutt, 2018). Cela peut être vrai à un stade expérimental. Mais,

une fois que la technologie est prête à être appliquée, il est essentiel de clarifier le statut juridique des transactions de la chaîne de blocs, et l'élaboration de la réglementation prend du temps. En outre, le calendrier n'est qu'un aspect du problème. Les questions de coordination et de contenu sont plus importantes. Comme les applications de la chaîne de blocs sont décentralisées et distribuées, elles concernent souvent plusieurs juridictions.

L'absence de coordination et d'accord sur la meilleure façon de réglementer la technologie de la chaîne de blocs au niveau international pourrait se solder par un enchevêtrement de règlements différents qui pourraient être plus nuisibles à terme que l'absence de règlement. La nature décentralisée et potentiellement mondiale de la chaîne de blocs nécessite une approche globale de la réglementation et, partant, des cadres de gouvernance appropriés (voir la section 4.2 d)).

(ii) Quels sont les lois et le cadre de responsabilité applicables ?

Les chaînes de blocs sans et avec permission soulèvent la question de la juridiction applicable, quoiqu'en des termes légèrement différents. Les unes et les autres peuvent s'étendre sur plusieurs juridictions, ce qui pose la question de savoir quelle loi nationale s'applique en cas de différend ou de fraude.

On pourrait faire valoir que chaque transaction relèverait de la juridiction du lieu où se trouve chaque participant au réseau. Toutefois, dans le cas des chaînes de blocs publiques, les nœuds peuvent se trouver n'importe où dans le monde, et en raison du caractère anonyme de la plate-forme, il est extrêmement difficile, voire presque impossible, d'identifier l'entité qui traite la transaction litigieuse et de déterminer précisément où celle-ci a lieu. Le problème est moins épineux dans le cas des chaînes de blocs avec permission, car les participants sont connus, mais la question de la juridiction applicable reste essentielle dans le cas de chaînes de blocs qui traversent plusieurs frontières juridiques.

De même, l'utilisation de la chaîne de blocs soulève des questions concernant le cadre de responsabilité applicable aux transactions de la chaîne de blocs en cas de problème, et le mécanisme de règlement en cas de conflit, de problèmes techniques ou d'action involontaire. En l'absence d'une entité centrale qui administre la plate-forme, qui est responsable du fonctionnement des registres distribués et des informations qu'ils contiennent en cas de différend ou d'action involontaire ayant des conséquences préjudiciables ? Et si un contrat intelligent ne fonctionne pas comme prévu, quelle partie est responsable ?

Ces obstacles réglementaires risquent-ils d'empêcher le déploiement de la technologie à grande échelle ? Dans le contexte des chaînes de blocs avec

permission, de nombreuses questions relatives à la juridiction et à la responsabilité peuvent avoir des solutions techniques. En fonction du cas concret et de la position des parties prenantes, une solution pourrait être d'avoir un contrat conventionnel « réel » qui régirait les relations entre les parties, couvrant à la fois ce que la chaîne de blocs est censée faire (par exemple, en permettant de demander des dommages-intérêts en cas de code erroné dans un contrat intelligent) et les aspects juridiques formels tels que la juridiction ou la loi applicables. Ce contrat, qui serait juridiquement contraignant, serait stocké dans la chaîne de blocs, de sorte que la version la plus récente serait disponible et immuable, sauf si les parties prenantes conviennent de modifications (en utilisant la fonction d'horodatage de la chaîne de blocs pour consulter la dernière version) (Deloitte, 2018). Néanmoins, dans certains cas – par exemple, dans le cas des lettres de crédit (voir aussi la section 3.1 a)), il peut être nécessaire d'établir des règles sectorielles définissant qui est responsable à chaque étape d'un processus particulier. Dans le cas des chaînes de blocs sans permission, les questions de la juridiction et de la responsabilité restent entières.

Outre l'incertitude réglementaire entourant l'utilisation des registres distribués, le déploiement de la chaîne de blocs à grande échelle pourrait également être entravé par diverses normes et prescriptions imposées par les autorités réglementaires nationales, y compris des prescriptions relatives à la localisation des données et des obstacles aux flux de données transfrontières.

(iii) Localisation et confidentialité des données

Ces dernières années ont été marquées par un intense débat sur les questions concernant la localisation des données, les restrictions au transfert de données transfrontières et la confidentialité des données, et un nombre croissant de pays ont adopté des mesures qui imposent des conditions ou des restrictions aux flux de données.

Selon la Information Technology and Innovation Foundation (ITIF), en mai 2017, 34 pays avait adopté ou proposé des prescriptions relatives à la localisation des données (Cory, 2017). Ces prescriptions peuvent prendre diverses formes. La localisation des données peut être expressément exigée par la loi ou elle peut résulter d'une série de restrictions qui rendent impossible *de facto* le transfert de données, en exigeant, par exemple, le stockage local ou le traitement local des données ou l'approbation du transfert de données par le gouvernement. Certains pays interdisent tout transfert de données, tandis que d'autres visent des secteurs ou des services particuliers. En ce qui concerne les obstacles aux flux de données transfrontières, il s'agit généralement de restrictions au transfert de données personnelles aux juridictions réputées offrir un moindre niveau de protection des données, et de limitations visant les renseignements que les gouvernements jugent « sensibles » (Cory, 2017).

Les gouvernements qui mettent en place des politiques de ce genre, lesquelles suscitent de plus en plus d'inquiétudes dans les milieux d'affaires en raison de leurs implications pour leurs activités, ont des motivations diverses. Les objectifs visés sont généralement de lutter contre les menaces pour la cybersécurité, de promouvoir l'économie locale, de garantir l'accès aux données aux fins de l'application de la loi et de protéger la vie privée des citoyens.

Dans quelle mesure les transactions de la chaîne de blocs peuvent-elles être affectées par de telles politiques ?

En tant que registres distribués, les plates-formes de chaîne de blocs ne sont guère affectées par les politiques de localisation des données. En effet, les exigences de stockage local et de traitement local des données, qui constituent la base de la plupart des politiques de localisation des données, sont automatiquement respectées : l'un des principes essentiels de la technologie de la chaîne de blocs est que tous les participants au réseau ont une copie locale des transactions et que chaque nœud participant pleinement doit traiter chaque transaction. Dès qu'une transaction est ajoutée à une chaîne de blocs, le registre numérique est mis à jour simultanément sur tous les nœuds. Par conséquent, l'objectif de faire en sorte que les données soient stockées et traitées localement est atteint automatiquement. Par contre, les prescriptions exigeant une approbation du gouvernement pour transférer des données auraient une incidence sur la capacité des participants potentiels dans les pays concernés de prendre part à un consortium de chaînes de blocs réunissant des acteurs de diverses juridictions.

En ce qui concerne la confidentialité des données, la chaîne de blocs est souvent présentée comme une opportunité ou un catalyseur pour assurer une plus grande protection des données personnelles et de nouvelles formes de gestion de l'identité. L'utilisation de divers outils cryptographiques permet aux utilisateurs de contrôler leurs données personnelles, et donc de les gérer et de les partager uniquement avec des parties de confiance.²⁷

Il convient de faire ici une distinction entre les chaînes de blocs publiques et les chaînes de blocs de consortium/privées. Une caractéristique particulière des chaînes de blocs publiques, comme Bitcoin, qui est souvent mise en avant, est qu'elles permettent des transactions entre les parties sans qu'aucune n'ait à révéler son identité à une autre partie ou au public. Alors qu'aujourd'hui, on ne peut généralement pas savoir qui traite nos données personnelles ni comment, les chaînes de blocs publiques permettent au sujet des données de rester anonyme ou d'utiliser un pseudonyme et de contrôler la façon dont ses données sont utilisées. Néanmoins, s'il est vrai qu'aucun renseignement personnel, comme le nom, l'adresse ou le numéro de téléphone, ne figure dans les entrées de données de la transaction

correspondante de la chaîne de blocs, une étude a montré qu'il était quand même possible de trouver l'adresse IP et donc de désanonymiser les clients – bien que le problème ne soit pas inhérent à la technologie et puisse être résolu en corrigeant la conception technique de la chaîne de blocs (Biryukov *et al.*, 2014).

Alors que les chaînes de blocs publiques permettent aux utilisateurs eux-mêmes d'appliquer le principe de la « confidentialité par conception » (Biryukov *et al.*, 2014) à un niveau individuel, les chaînes de blocs de consortium/privées reprennent ce principe au niveau de la plate-forme : le degré de confidentialité est déterminé par la gestion de la plate-forme. Sur de telles plates-formes, les participants sont connus et identifiés, mais les permissions de lire et d'écrire certaines des données ajoutées à la plate-forme peuvent être réservées à certains participants afin de protéger la confidentialité (voir la section 2.3). Ce qui est clair, c'est que les entités qui utilisent une plate-forme basée sur la chaîne de blocs doivent veiller à ce que la conception technique de la plate-forme respecte les prescriptions du ou des cadre(s) réglementaire(s) pertinent(s), notamment des lois sur la protection des données.

Le déploiement de la technologie pourrait toutefois être limité par les droits accordés aux individus en vertu des règlements nationaux sur la protection des données. On a beaucoup parlé, par exemple, de la possible incompatibilité entre le Règlement général sur la protection des données (RGPD) de l'UE, qui est entré en vigueur le 25 mai 2018, et la chaîne de blocs, ce qui a amené certains à se demander si le RGPD ne risquait pas finalement de « bloquer la chaîne de blocs » (Toth, 2018).

En effet, deux dispositions clés du RGPD semblent à priori incompatibles avec la chaîne de blocs, à savoir le « droit de rectification » et le « droit à l'oubli » – c'est-à-dire le droit de rectifier des données personnelles ou d'obtenir leur suppression (articles 16 et 17 du RGPD). En raison de la nature immuable des chaînes de blocs, il est très difficile de mettre à jour, de supprimer, de modifier ou de corriger des données. Certains membres de la communauté soutiennent qu'une solution pourrait être de conserver les données personnelles hors de la chaîne, en ne faisant apparaître dans la chaîne que la preuve de la transaction (le hash cryptographique*), ce qui préserverait son intégrité tout en permettant de supprimer la transaction elle-même (Deloitte, 2017 ; IBM, 2018). La suppression des données conservées à l'extérieur de la chaîne signifierait que le hash stocké sur la chaîne de blocs désignerait un emplacement supprimé. D'autres notent cependant que les données hachées sont considérées comme des données personnelles dans le cadre de la législation de l'UE (Finck, 2017).

Certains observateurs ont également noté que, si les chaînes de blocs et le RGPD semblent incompatibles au niveau conceptuel, les deux ont le même objectif, à

savoir donner aux individus plus de contrôle sur leurs données personnelles, mais par des mécanismes différents. On pourrait examiner la question de savoir si les objectifs sous-jacents du RGPD pourraient être atteints par des moyens autres que ceux qui étaient envisagés à l'origine (Finck, 2017). Il est intéressant de noter que les fonctions de suivi et de contrôle intégrées à la chaîne de blocs pourraient aider les organisations à se conformer plus facilement à une autre disposition du RGPD exigeant la tenue de registres internes. Bien que le RGPD n'ait a priori aucun rapport direct avec le commerce international, puisque la plupart des renseignements contenus dans les documents commerciaux concernent des entreprises et non des personnes physiques, il pourrait avoir un impact sur le commerce dans certains cas, lorsque les coordonnées d'une personne dans une entreprise doivent être fournies (par exemple pour l'exportation de marchandises dangereuses). À terme, la nécessité de trouver un compromis entre la protection juridique des données personnelles et l'encouragement de l'innovation est une question que les régulateurs devront peut-être aborder, et qui souligne la nécessité de mettre en place des instances de gouvernance appropriées.

(iv) Comblent le fossé entre le monde de la loi et le monde du code

Bien que la relation entre le monde de la loi et le monde du code ait beaucoup évolué depuis l'avènement des technologies numériques, avec la numérisation du droit et l'émergence du concept «le code fait loi», popularisé par Lawrence Lessig (Lessig, 1999) (c'est-à-dire l'idée que le code fixe les conditions régissant le comportement des internautes), la loi demeure difficile à lire pour les machines mais facile à appréhender pour les humains. À l'inverse, les codes utilisés pour programmer les machines et les contrats intelligents sont particulièrement obscurs et complexes pour les humains.

Le comblement du fossé entre le monde de la loi et le monde du code, s'il n'est pas une condition préalable au déploiement de la chaîne de blocs, pourrait faciliter grandement l'utilisation des contrats intelligents. La législation et les contrats sont souvent rédigés pour un monde basé sur le papier, d'une manière qui les rend difficiles à utiliser dans les contrats numériques. Une nouvelle approche de la réglementation est en train de voir le jour, qui préconise la «codification de la loi» (De Filippi et Hassan, 2018). Diverses organisations et start-up examinent comment la loi pourrait être codifiée et rendue lisible par machine afin de faciliter la transposition des obligations contractuelles dans un code contractuel numérique. La Nouvelle-Zélande a récemment réalisé un projet visant à examiner comment les lois pourraient être réécrites et formulées programmiquement afin de pouvoir être analysées par une machine (Darabi, 2018), et plusieurs start-up, comme Monax²⁸ et ContraxSuite²⁹, offrent des services d'«ingénierie juridique» pour aider à codifier les

obligations contractuelles et à les rendre lisibles par machine, afin de faciliter la rédaction de contrats intelligents.

Alors que le passage de la notion «le code fait loi» à la notion «la loi est le code» (c'est-à-dire la loi définie comme un code) pourrait permettre d'importants gains d'efficacité et de transparence et faciliter l'utilisation des contrats intelligents, la difficulté de transposer la flexibilité des règles juridiques dans un langage formalisé pouvant être interprété et utilisé par des machines peut aussi conduire à plus de rigidité dans l'application des règles (De Filippi et Hassan, 2018). Il est essentiel de trouver un juste équilibre entre une plus grande efficacité grâce à la lisibilité par machine et la flexibilité.

(v) Identification juridique des entreprises

Quand une transaction a lieu, il est indispensable de pouvoir identifier convenablement les contreparties. L'identification juridique est plus importante, mais aussi plus problématique, dans un monde où de nombreuses transactions commerciales et financières sont internationales et couvrent plusieurs juridictions qui n'appliquent pas forcément les mêmes normes, en particulier quand les transactions ont lieu en quelques nanosecondes, comme c'est le cas dans le secteur financier. La nécessité d'une approche cohérente a été mise en évidence par la crise financière de 2008, qui a révélé des problèmes fondamentaux dans les systèmes existants concernant l'identification des entités, ce qui a mené le G-20 à demander la création d'un identifiant d'entité juridique mondial (LEI)³⁰ – c'est-à-dire un cadre mondial pour l'identification juridique des acteurs économiques participant aux transactions financières.³¹

Bien qu'elle ne soit pas indispensable pour mettre en œuvre les applications de la chaîne de blocs, l'existence d'un LEI mondial faciliterait grandement le traitement des transactions basées sur la chaîne de blocs et permettrait d'utiliser plus efficacement la technologie. Les efforts faits actuellement pour concevoir un système mondial sont bienvenus, mais une plus grande coordination internationale est nécessaire pour éviter la création de systèmes distincts. En effet, le LEI mondial s'applique aux entités juridiques participant aux transactions financières. En parallèle, des discussions ont lieu à l'OMD pour créer un numéro d'identification mondial des négociants. Assurer la cohérence de ces deux approches ou unir les efforts pour créer un système commun apporterait des avantages évidents aux entités participant aux transactions commerciales internationales et favoriserait le déploiement de technologies telles que la chaîne de blocs, qui ont le potentiel d'améliorer de manière significative les processus commerciaux. Inversement, l'utilisation de la chaîne de blocs pourrait être intéressante pour soutenir les efforts visant à développer des systèmes mondiaux d'identification des entités.

(d) Questions de gouvernance

Si la chaîne de blocs est une technologie prometteuse, elle ne pourra être déployée à grande échelle que si les problèmes techniques, juridiques et d'interopérabilité sont réglés de manière coordonnée aux niveaux technique et politique appropriés. Pour le moment, le monde de la chaîne de blocs et des cryptomonnaies s'apparente au «Far West». Il faut un système de gouvernance bien pensé³², qui aborde les questions de normalisation et les questions juridiques et politiques, tout en assurant la souplesse nécessaire pour permettre à la technologie de se développer.

Pour beaucoup, l'approche multipartite qui régit Internet constitue un modèle de gouvernance intéressant. La gouvernance d'Internet repose sur une série de «réseaux de gouvernance mondiaux» qui réunissent des entreprises, des organisations de la société civile, des développeurs de logiciels, des universitaires et des gouvernements. Ces réseaux, qui fonctionnent par consensus, sont de sept types (Tapscott et Tapscott, 2017) :

1. Les réseaux normatifs, qui sont des organisations non étatiques à but non lucratif chargées d'élaborer des spécifications et des normes techniques, telles que l'Internet Engineering Task Force (IETF), organisme de normalisation ouvert qui élabore et promeut des normes Internet volontaires.
2. Les réseaux de connaissances, qui font de la recherche et proposent de nouvelles idées pour aider à résoudre des problèmes mondiaux, comme l'Internet Research Task Force (IRTF).
3. Les réseaux d'attribution, comme l'International Corporation for Assigned Names and Numbers (ICANN), qui est un partenariat public-privé qui attribue les noms de domaine Internet et qui œuvre au maintien de la stabilité opérationnelle d'Internet.
4. Les réseaux d'orientation politique, qui éclairent le débat sur les politiques et contribuent à leur élaboration, comme le Internet & Jurisdiction Policy Network, qui facilite la coopération transnationale sur la cybersécurité, les droits de l'homme et les autres politiques juridiques et économiques.
5. Les réseaux de plaidoyer, qui cherchent à influencer l'agenda ou les politiques des gouvernements, des entreprises et d'autres institutions, comme l'Industrial Internet Consortium, groupe de chercheurs, d'entreprises et d'organismes publics qui soutient l'adoption d'applications d'Internet dans différents secteurs pour accélérer le développement de l'Internet des objets.
6. Les réseaux de surveillance.
7. Les institutions en réseau, comme l'Internet Society, qui se définit comme une organisation «mondiale axée sur les causes» qui s'attache à faire en sorte qu'Internet reste «ouvert, connecté et sécurisé au niveau mondial». ³³ L'Internet Society est gouvernée par un conseil d'administration composé de représentants

des milieux d'affaires, du monde universitaire et du secteur à but non lucratif. Le Forum sur la gouvernance de l'internet est une autre institution en réseau dont la création a été officiellement annoncée par le Secrétaire général de l'Organisation des Nations Unies en juillet 2006. Le Forum sert de cadre à un dialogue multipartite sur les questions de politique publique liées à la gouvernance d'Internet, telles que la durabilité, la robustesse, la sécurité, la stabilité et le développement d'Internet.

Certains groupes et réseaux axés sur la chaîne de blocs commencent à voir le jour, comme le Blockchain Research Institute³⁴ et la Blockchain Interoperability Alliance, un groupe de plaidoyer qui vise à élaborer des normes acceptées au niveau mondial pour promouvoir une meilleure connectivité et une plus grande interopérabilité entre les différents réseaux de chaîne de blocs (Higgins, 2017a). En outre, diverses organisations internationales mettent en place des comités et des groupes de travail pour examiner la technologie, notamment l'ICC, l'ISO, l'UIT, le CEFAC-ONU et l'OMD. En mars 2017, le FMI a créé un groupe consultatif de haut niveau sur la technologie financière, composé de directeurs de banques, d'entreprises de la chaîne de blocs, d'organismes de régulation et d'universitaires, et chargé d'étudier les implications économiques et réglementaires de la technologie de la chaîne de blocs (FMI, 2017). Un comité de l'ISO a été créé en 2016 pour élaborer des normes afin de permettre une « meilleure interopérabilité, une adhésion plus rapide et davantage d'innovation dans [l']usage et [l']application » de la technologie de la chaîne de blocs. Plus récemment, en février 2018, la Commission européenne a annoncé le lancement d'un Observatoire-forum des chaînes de blocs de l'UE. Il s'agit d'un forum ouvert pour les spécialistes de cette technologie, les innovateurs, les citoyens, les parties prenantes du secteur, les pouvoirs publics, les autorités de régulation et de surveillance, où ils pourront débattre et élaborer de nouvelles idées et orientations. Il collectera des informations, suivra et analysera les tendances et examinera le potentiel socioéconomique des chaînes de blocs et la meilleure façon de relever les défis (Commission européenne, 2018).

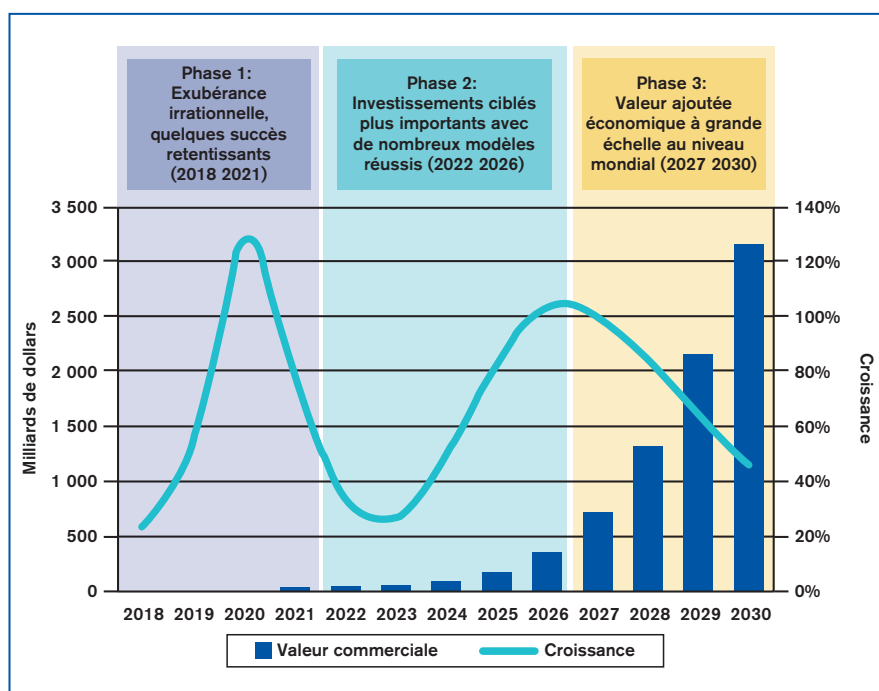
Mais il n'existe pas encore d'écosystème complet rassemblant les entreprises, les organisations de la société civile, les développeurs de logiciels, les universitaires, les gouvernements et les organisations inter-gouvernementales dans différents contextes pour examiner les questions de normalisation et les questions juridiques et politiques. Le manque de coordination à un niveau supranational entre les différentes parties prenantes pourrait freiner le déploiement de la technologie.

Il convient de se demander s'il serait utile d'engager un débat sur les implications pratiques et juridiques de la chaîne de blocs dans les organisations internationales pertinentes telles que l'OMC, afin d'aider à mieux comprendre les avantages potentiels de la technologie, ainsi que ses limites et les défis qui peuvent apparaître

si elle est déployée plus largement. Comme le montrent les divers exemples cités dans cette publication, le secteur privé avance à toute allure. Étant donné que cette technologie pourrait avoir un impact considérable sur les transactions commerciales internationales, il est important que les autorités de régulation commencent à réfléchir aux moyens de soutenir le déploiement de la technologie.

Comme l'a montré ce chapitre, les avantages potentiels de la chaîne de blocs pour le commerce international sont multidimensionnels. En facilitant le suivi des produits tout au long de la chaîne d'approvisionnement, la chaîne de blocs peut contribuer à accroître la confiance et la transparence dans les chaînes de valeur. Elle peut réduire considérablement un certain nombre de coûts du commerce et elle peut offrir de nouvelles possibilités aux MPME, en particulier aux petits producteurs des pays en développement, pour accéder aux marchés mondiaux.

Figure 19 Prédiction de la valeur commerciale des chaînes de blocs



Source: Figure 3 : « Blockchain Business Value Forecast Highlights Three Phases of Development », dans Gartner (2018).

Néanmoins, plusieurs défis doivent être relevés pour que la technologie puisse être déployée à grande échelle et puisse avoir un effet transformateur ; il s'agit notamment des problèmes de scalabilité et d'interopérabilité et des questions réglementaires.

Les défis à relever sont à la hauteur des possibilités qu'offre la technologie. Pour le moment, il est difficile de savoir où elle nous mènera à terme. Nous sommes, comme le note Gartner (2018), dans une phase « d'exubérance irrationnelle, avec quelques succès retentissants » (voir la figure 19). Il faudra probablement encore quelques années et beaucoup d'autres preuves de concept et de projets pilotes avant que des modèles réussis voient le jour et que le potentiel réel de la technologie et son impact tangible sur le commerce international puissent être pleinement évalués. Mais, étant donné l'effet transformateur qu'elle pourrait avoir sur le commerce mondial, il est essentiel de comprendre les implications pratiques et juridiques de la chaîne de blocs pour le commerce international et d'essayer de trouver des solutions collectives aux problèmes actuels.

Note de fin

1. Voir <https://www.agridigital.io/>.
2. Voir <https://www.provenance.org/case-studies/co-op>.
3. Voir <http://www.carrefour.com/news/4-new-food-quality-commitments>.
4. Voir <https://www.provenance.org/case-studies/martine-jarlggaard>.
5. Discussion avec des responsables de Walmart.
6. Voir <https://www.provenance.org/tracking-tuna-on-the-blockchain>.
7. Voir <https://www.provenance.org/case-studies/fairfood>.
8. Voir <http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade>.
9. Les organisations nationales et internationales qui ont mené des enquêtes axées sur les MPME sont notamment le Centre du commerce international (ITC), la Commission du commerce international des États-Unis (USITC), la Commission européenne, la Banque mondiale, l'OCDE et l'OMC. Pour une synthèse récente des obstacles rencontrés par les MPME, voir OMC (2016c).
10. Voir <https://www.fasttracktrade.co>.
11. Voir <https://cambodia.oxfam.org/what-we-do-resilience/blockchain-livelihoods-organiccam-bodian-rice-blocrice-project>.
12. Voir <https://sustainabledevelopment.un.org/sdg9>.

13. Voir <https://blockchain.info/de/charts/transactions-per-second?timespan=1year>.
14. Voir <https://etherscan.io/chart/tx>. La limite des blocs d'Ethereum n'est pas calculée simplement à partir de la taille du bloc – comme dans le cas de Bitcoin. À chaque transaction sur Ethereum correspond une quantité de «gaz» déterminée. Le «gaz» désigne la redevance payée pour l'exécution de chaque opération réalisée sur Ethereum. Son montant est exprimé en ether et est défini par les mineurs. Chaque bloc d'Ethereum a une «limite de gaz», qui est déterminée par un algorithme et par le vote des mineurs et qui varie d'un bloc à l'autre. La «limite de gaz» pour chaque bloc détermine le nombre de transactions qu'il peut contenir. En théorie, Bitcoin et Ethereum ont une capacité de plus de 1 000 transactions par seconde.
15. Pour une présentation détaillée et relativement peu technique des solutions proposées, voir <https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a>.
16. Voir, par exemple, "Future of Blockchain: Will Hashgraph make Blockchain obsolete?", TechStartup blog, 14 mars 2018. Adresse consultée : <https://techstartups.com/2018/03/14/future-ofblockchain-will-hashgraph-make-blockchain-obsolete/> consultée le 8 mai 2018.
17. Pour une note technique sur les solutions d'interopérabilité des chaînes, voir Buterin (2016).
18. Voir <https://sawtooth.hyperledger.org/docs/core/releases/1.0/introduction.html> et <https://www.hyperledger.org/projects/hyperledger-burrow>.
19. Voir <https://www.hyperledger.org/projects/quilt>. Le projet Hyperledger Quilt a été mis au point pour appliquer la norme de paiement inter-registres élaborée par le World Wide Web Consortium (W3C).
20. Voir <https://www.unece.org/?id=3133>.
21. Voir <http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/data-model.aspx>.
22. Voir <https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx>.
23. La présente étude porte sur les cas d'utilisation de la chaîne de blocs, et non sur les cryptomonnaies. Il faut noter cependant que le statut juridique des cryptomonnaies varie aussi beaucoup d'un pays à l'autre. Alors que certains pays ont expressément autorisé l'utilisation des bitcoins, d'autres l'ont restreinte ou interdite. Dans un article récent évaluant les différences de statut des cryptomonnaies entre les juridictions nationales, Chohan (2017) note que si la plupart des pays ne rendent pas illégale l'utilisation des cryptomonnaies, le statut exact de ces monnaies reste indéfini ou changeant dans de nombreux pays. La diversité des approches législatives «indique d'une part la perplexité des autorités quant aux pleines possibilités des cryptomonnaies, et d'autre part une prise de conscience de l'inadéquation du rôle de surveillance et de gouvernance qui serait le leur eu égard au caractère désintermédié des transactions en cryptomonnaies» Chohan (2017). La nature décentralisée de la chaîne de blocs rend les autorités au mieux perplexes, et souvent préoccupées quant à leur rôle et leur pertinence dans le processus.
24. En 2015, par exemple, le FinCEN, bureau de lutte contre la criminalité financière des États-Unis, a engagé une action au civil contre Ripple, accusant la start-up de ne pas s'être fait enregistrer en tant qu'entreprise de services monétaires réglementée. Cité dans Werbach (2018).
25. Voir <https://www.legifrance.gouv.fr/eli/ordonnance/2017/12/8/2017-1674/jo/texte>.

26. L'Initiative conjointe sur le commerce électronique a été lancée en marge de la onzième Conférence ministérielle (CM11) en décembre 2017 par des ministres représentant 71 Membres de l'OMC. Dans la déclaration, les signataires sont convenus d'engager ensemble des travaux exploratoires en vue de négociations futures à l'OMC sur les aspects du commerce électronique liés au commerce. Voir, en particulier, les propositions présentées par le Brésil (document JOB/GC/176), l'Union européenne (document JOB/GC/188), le Japon (documents JOB/GC/177 et JOB/GC/180), la Nouvelle-Zélande (document JOB/GC/175), la Fédération de Russie (document JOB/GC/181), Singapour (document JOB/GC/179) et les États-Unis (JOB/GC/178) (à la mi-avril 2018).

27. Voir Sullivan et Burger (2017). Pour un aperçu, voir aussi <https://blockchainhub.net/blog/blog/decentralized-identity-blockchain/>.

28. Voir <https://monax.io>.

29. Voir <https://contraxsuite.com>.

30. Pour une présentation de l'identifiant d'entité juridique mondial, voir <https://www.gleif.org/fr/about-lei/introducing-the-legal-entity-identifier-lei>.

31. «Nous soutenons la création d'un identifiant international pour les entités juridiques (legal entity identifier – LEI), qui identifie de manière unique les contreparties aux transactions financières. Nous invitons le CSF à prendre l'initiative en aidant à coordonner les travaux de la communauté des régulateurs afin d'élaborer, d'ici au prochain sommet, des recommandations sur la mise en œuvre d'un cadre de gouvernance approprié, tenant compte de l'intérêt général, pour cet identifiant international.» Déclaration du Sommet du G-20 tenu à Cannes en 2011, <http://www.g20.utoronto.ca/2011/2011-cannes-declaration-111104-fr.html>.

32. Certains développeurs préfèrent le terme «administration» parce qu'ils estiment que le terme «gouvernance» donne l'impression qu'un élément pose problème et doit être corrigé.

33. Voir <https://www.internetsociety.org/fr/>.

34. Voir <https://www.blockchainresearchinstitute.org/>.

5 Conclusion

Le monde tel que nous le connaissons aujourd'hui a été façonné par les innovations technologiques. Une nouvelle technologie, la chaîne de blocs – technologie de registres distribués –, a été accueillie par beaucoup avec enthousiasme et optimisme comme le prochain grand facteur de changement. La chaîne de blocs, qui permet de diffuser des données et des informations numériques de manière sûre, transparente et immuable sans avoir à recourir à un tiers de confiance unique, est une technologie particulièrement prometteuse. Elle pourrait permettre aux individus et aux entreprises du monde entier d'effectuer des transactions de manière plus efficace, plus économique et plus rapide, tout en conservant un haut niveau de sécurité. Elle pourrait avoir un impact considérable sur la façon de réaliser les opérations commerciales, qu'il s'agisse des transactions financières ou des transactions commerciales transfrontières physiques, en réduisant les coûts de traitement, de vérification, de suivi, de coordination et de transport grâce à la simplification et à la numérisation des processus qui impliquent de multiples parties prenantes et qui étaient, jusqu'à présent, fortement tributaires du papier. Elle pourrait réduire la fraude, permettre une meilleure administration des droits de propriété intellectuelle, renforcer la traçabilité et la confiance dans les chaînes de valeur et offrir de nouvelles possibilités aux petites entreprises.

Les précédentes innovations technologiques – de la vapeur à l'électricité et, plus récemment, à Internet – ont bouleversé l'organisation de la production et la communication. La chaîne de blocs peut avoir un impact sur les transactions, comparable à l'impact d'Internet sur la communication. Parfois appelée l'internet des valeurs», la chaîne de blocs est avant tout l'«internet des transactions». En supprimant les cloisons qui existent actuellement entre les nombreuses parties aux transactions commerciales transfrontières, la chaîne de blocs pourrait porter la mondialisation du commerce à un autre niveau.

Toutefois, la chaîne de blocs n'est pas adaptée à toutes les situations et n'est pas une solution à tous les problèmes. Cette technologie fonctionne de manière optimale dans les cas où de multiples parties sont impliquées dans des transactions qui nécessitent de la confiance et de la transparence. Si son utilisation est pertinente dans de nombreuses situations, la chaîne de blocs peut créer des obstacles si elle

est utilisée pour des transactions qui ne nécessitent pas un niveau élevé de fiabilité. En outre, l'établissement d'une chaîne de blocs exige des efforts d'investissement et de coordination importants, et de profonds changements systémiques et culturels. Il est essentiel de peser avec soin le pour et le contre.

Plus important encore, la technologie est encore en train d'évoluer et de nombreux défis, notamment des défis techniques et juridiques et des questions d'interopérabilité, doivent être résolus avant que le potentiel de la technologie puisse être pleinement exploité. Il importe, en particulier, de trouver des solutions techniques pour remédier au problème des «îlots numériques» et faire en sorte que les chaînes de blocs puissent communiquer entre elles, et d'établir des règles pour clarifier les lois applicables et réglementer les responsabilités. Sans ce volet réglementaire, la chaîne de blocs pourrait être confinée aux preuves de concept et aux projets pilotes.

Il est difficile de dire où nous mènera l'aventure de la chaîne de blocs. Faut-il s'attendre à une refonte complète de nos économies à court ou moyen terme à cause des registres distribués ? Probablement pas. Une approche hybride, dans laquelle les registres distribués complètent les systèmes existants, est plus probable. La technologie elle-même continue d'évoluer et pourrait être assez différente dans quelques années. De nouvelles technologies de registres distribués d'un niveau «supérieur» voient déjà le jour. Elles sont plus rapides, plus sûres et plus économes en énergie que la chaîne de blocs initiale. Que l'avenir de cette technologie soit la chaîne de blocs telle qu'elle a été conçue à l'origine ou une autre technologie de registres distribués plus performante, une chose est sûre : la technologie mérite d'être étudiée, et pour qu'elle puisse réaliser son plein potentiel, il faut trouver des solutions collectives qui répondent aux principaux défis existants tout en laissant la flexibilité nécessaire pour que la technologie puisse se développer.

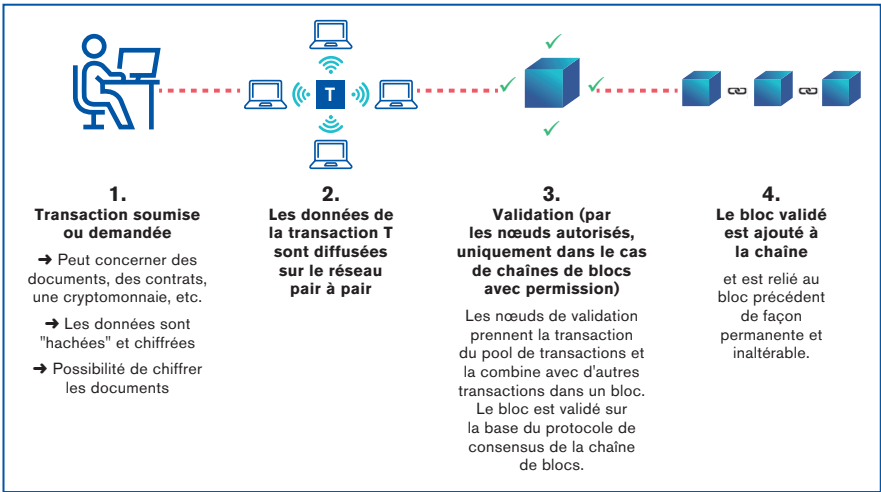
Compte tenu du potentiel de la chaîne de blocs, les entreprises, les organisations de la société civile, les développeurs de logiciels, les universitaires, les gouvernements et les organisations inter-gouvernementales devraient travailler main dans la main pour évaluer les implications pratiques et juridiques de la technologie et trouver des solutions collectives aux défis existants. Cela est particulièrement vrai dans le cas du commerce international. La chaîne de blocs pourrait rendre le commerce international plus intelligent, mais un commerce intelligent nécessite une normalisation intelligente, laquelle ne peut exister que grâce à la coopération. Si nous parvenons à créer un écosystème favorable au développement plus large de la chaîne de blocs, le commerce international pourrait bien être radicalement différent dans 10 ou 15 ans.

Annexe – La chaîne de blocs pour les fans de technologie

Comment fonctionne la chaîne de blocs?

La chaîne de blocs n'est que l'un des types de technologie des registres distribués (DLT). Cette technologie évolue rapidement et de nouveaux modèles de flux de transactions sont développés actuellement pour améliorer la rapidité et la sécurité et réduire la consommation d'énergie. Ces modèles s'éloignent du concept de « blocs », et parfois à la fois des concepts de « chaîne » et de « blocs ». Ces nouveaux venus sont notamment IOTA, Ripple et Hashgraph. Bien qu'il ne s'agisse pas de chaînes de blocs proprement dites, l'expression « chaîne de blocs » est couramment employée pour désigner plus généralement la technologie des registres distribués et le phénomène qui l'accompagne. La figure A.1 illustre les étapes typiques des transactions dans la chaîne de blocs. Bien que cette section fasse une distinction entre la chaîne de blocs et les autres technologies de registres distribués afin d'en expliquer les différentes étapes et de clarifier les concepts, l'expression « chaîne de blocs » est utilisée dans cette étude pour désigner plus généralement la technologie des registres distribués.

Figure A.1 Étapes typiques d'une transaction dans la chaîne de blocs



Source: Auteure.

Étape 1 :

L'expéditeur soumet ou demande une transaction. Une transaction dans la chaîne de blocs/DLT peut concerner n'importe quel type d'actif – qu'il soit numérique (cryptomonnaie, peinture numérique, par exemple), corporel (transfert de propriété ou de fonds, ou échange de documents tels qu'une déclaration en douane ou un certificat d'origine, par exemple) ou incorporel (prestation de service, par exemple) – qui est échangé entre les participants au réseau. La transaction peut concerner des documents, des contrats, des cryptomonnaies, ou tout autre type d'actif.

Lorsqu'une transaction est soumise, divers processus ont lieu pour garantir la sécurité de la transaction :

- Premièrement, l'expéditeur génère une paire de clés, comprenant une clé publique et une clé privée. Ces clés sont mathématiquement liées. La clé publique est mise à la disposition du destinataire.
- L'expéditeur hache* ensuite les données à envoyer, c'est-à-dire qu'il les convertit en une nouvelle chaîne numérique d'une longueur prédéfinie et fixe au moyen d'une fonction mathématique – un «hash». Le hachage assure l'intégrité des données et empêche la falsification.¹ La valeur de hachage obtenue est chiffrée* au moyen de la clé privée de l'expéditeur. Le hash chiffré constitue la signature numérique* des données, c'est-à-dire l'empreinte numérique d'un document électronique. Il garantit que le message a été créé et envoyé par l'expéditeur déclaré et n'a pas été modifié pendant le transit. L'expéditeur ne peut pas nier avoir envoyé le message.
- L'expéditeur transmet ensuite la signature numérique avec les données en clair aux participants au réseau pair à pair – les destinataires.

Si l'expéditeur ne souhaite pas que les autres participants au réseau voient le contenu du message, c'est-à-dire les données en clair contenues dans les documents soumis, il peut choisir de chiffrer le message.

Étape 2 :

Une fois que la signature numérique a été générée et que le message a été haché et chiffré, il est transmis aux participants au réseau pair à pair – les destinataires, également appelés nœuds* – et ajouté à un pool de transactions non validées.

Étape 3 : Validation

Le processus de validation diffère selon le type de DLT et le protocole de consensus propre à la chaîne de blocs ou à la DLT.

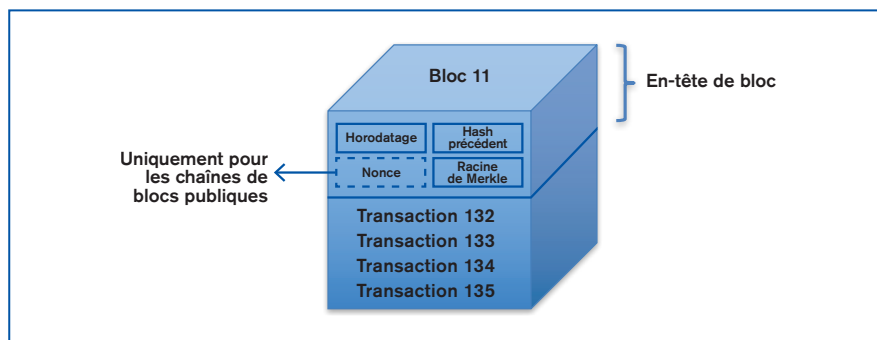
Les destinataires – dans le cas des chaînes de blocs avec permission, les nœuds autorisés – valident la transaction en utilisant la clé publique de l'expéditeur pour déchiffrer la transaction. Un déchiffrement réussi confirme que la transaction provient de l'expéditeur déclaré. Le destinataire peut alors vérifier l'intégrité des données en comparant la valeur de hachage déchiffrée envoyée par l'expéditeur avec celle qu'il a calculée en appliquant le même algorithme de hachage aux données en clair transmises par l'expéditeur. Si les deux valeurs de hachage coïncident, le destinataire a la garantie que les données n'ont pas été modifiées pendant le transit. La transaction peut alors être validée.

La chaîne est ensuite mise à jour via le «protocole de consensus». Les protocoles de consensus permettent de classer les transactions et les blocs de manière uniforme et claire, et garantissent l'intégrité et la cohérence de la chaîne de blocs entre des nœuds répartis géographiquement (voir plus loin la présentation des protocoles de consensus les plus fréquemment utilisés).

Dans le cas de la technologie de la chaîne de blocs, les transactions validées sont d'abord combinées à d'autres transactions pour créer un bloc, qui est ensuite validé² sur la base du protocole de consensus de la chaîne de blocs. S'il est validé, le nouveau bloc est relié à la chaîne en tant qu'«état réel du registre». Chaque bloc contient plusieurs transactions (voir la figure A.2). Un bloc est composé d'un en-tête de bloc et d'entrées de transactions. L'en-tête de bloc contient les éléments suivants :

- Le numéro du bloc.
- L'horodatage* actuel qui indique la date et l'heure pour assurer l'enregistrement de la séquence chronologique.
- Le hash du bloc précédent – aussi appelé pointeur de hachage – pour relier les blocs entre eux.
- Le hash de ce que l'on appelle la «racine de Merkle»*, qui permet de comparer et de vérifier facilement de grands ensembles de données de transactions sans avoir à inclure l'ensemble complet des données de chaque transaction dans l'en-tête du bloc, ce qui fait que la taille des blocs est plus facile à gérer.

En outre, pour les chaînes de blocs publiques comme le bitcoin, l'en-tête de bloc inclut le «nonce»* – c'est-à-dire une séquence de nombres aléatoire que les mineurs* doivent trouver afin de valider le bloc et le niveau de difficulté qui lui est associé.

Figure A.2 Composition d'un bloc

Source : Auteure.

Étape 4 :

Une fois qu'un bloc est validé ou, dans le cas des DLT qui ne combinent pas les transactions en blocs, une fois que la transaction a été validée, le bloc ou la transaction est horodaté(e) et relié(e) aux blocs précédents ou aux transactions précédentes par un «pointeur de hachage» – un hash du bloc précédent/de la transaction précédente – ce qui forme une chaîne chronologique linéaire de blocs/de transactions.

Les transactions sont ensuite confirmées et le bloc/la transaction ne peut plus être modifié(e) ou supprimé(e) – le bloc ou la transaction est donc immuable. Chaque fois qu'un bloc ou qu'une transaction est ajouté(e) à la chaîne, le registre numérique est mis à jour sur tous les nœuds participants. La mise à jour systématique du registre sur tous les nœuds est un moyen efficace de s'assurer qu'il n'existe pas de versions divergentes du registre dans les nœuds participants.

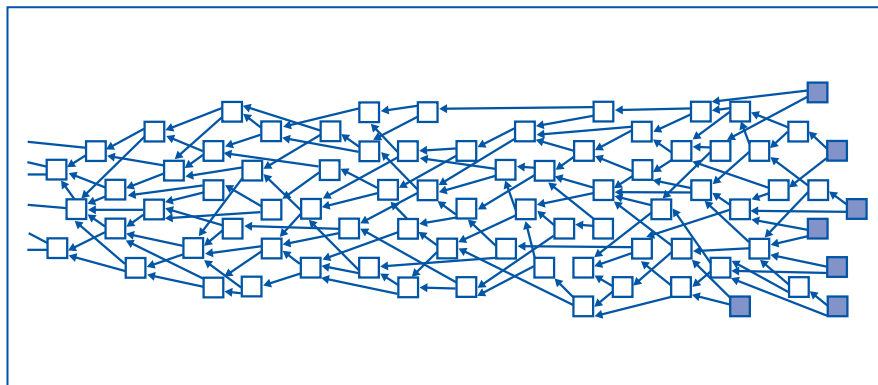
D'autres technologies de registres distribués suivent un processus différent. Dans IOTA, par exemple, les transactions ne sont pas groupées en blocs et chaque transaction est reliée aux deux transactions précédentes dans le cadre du processus de validation pour former un «Tangle» (entrelacs) (voir la figure A.3).

Qu'est-ce qui rend la chaîne de blocs si différente?

Alors que la sécurité de l'information a reposé, pendant plusieurs décennies, sur les différentes techniques décrites ci-dessus (signatures numériques, hachage, chiffrement, arbres de Merkle), leur résistance aux attaques malveillantes n'a cessé d'être remise en question, ce qui a conduit les pirates et les spécialistes de la cybersécurité à jouer indéfiniment au chat et à la souris pour développer des codes

et les décrypter. Des progrès ont été accomplis, sans avancée majeure jusqu'à la création de la technologie de la chaîne de blocs.

Figure A.3 Le Tangle

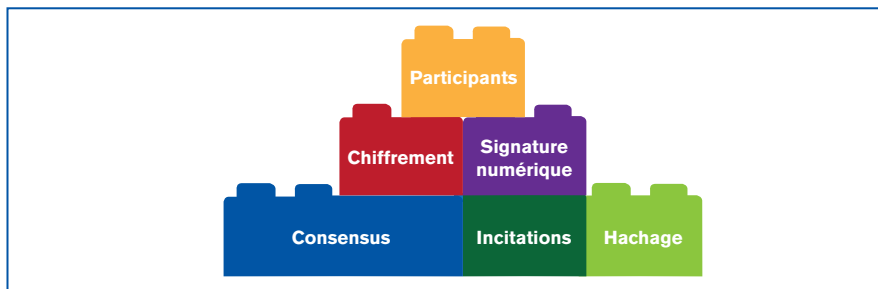


Source: IOTA.³

La principale innovation de la chaîne de blocs est qu'elle a combiné les propriétés de toutes ces technologies et apporté aux protocoles des modifications mineures, bien réfléchies afin de renforcer la sécurité. Tout comme les briques Lego, différentes briques peuvent être prises et assemblées de différentes façons pour créer des fonctions spécifiques (voir la figure A.4) (voir Lewis, 2015).

Le caractère immuable de la chaîne de blocs – le fait que les données ne peuvent pas être facilement modifiées ou supprimées après validation – est obtenu en utilisant les diverses propriétés des algorithmes de hachage et des pointeurs de hachage. Cependant, au lieu de simplement contenir l'adresse du bloc précédent (comme dans les protocoles classiques), les pointeurs de hachage de la chaîne de

Figure A.4 Les «blocs élémentaires» de la chaîne de blocs



Source: Auteur.

blocs contiennent le hash des données contenues dans le bloc précédent. En conséquence, à la différence des bases de données distribuées traditionnelles, toute modification des données d'un bloc entraînera une modification de tous les blocs précédents. Ce petit changement est à l'origine de l'immuabilité de la chaîne de blocs. C'est également ce qui rend la chaîne de blocs extrêmement fiable.

De plus, la chaîne de blocs remplace l'horodatage de confiance par une alternative distribuée et inviolable. Lorsqu'un bloc est validé et ajouté à la chaîne, l'horodatage fournit une preuve sûre de l'heure exacte à laquelle ces données ont été ajoutées et ont existé.

Quelques protocoles de consensus couramment utilisés

Preuve de travail (PoW – Bitcoin)

Ce protocole de consensus est utilisé par Bitcoin et plusieurs autres plates-formes de cryptomonnaie publiques. La preuve de travail exige que les participants qui valident les blocs – en d'autres termes les validateurs, aussi appelés « mineurs » – démontrent qu'ils ont utilisé une puissance de calcul considérable pour résoudre un puzzle cryptographique compliqué (problème mathématique basé sur la règle du consensus). Ce processus s'appelle le « minage »*. Les mineurs sont en concurrence pour valider un bloc et l'ajouter à la chaîne de blocs. Pour ce faire, ils produisent un nombre suffisant de suppositions aléatoires sur leur ordinateur pour résoudre le puzzle cryptographique. Les mineurs ont une incitation financière à traiter le plus grand nombre de transactions le plus rapidement possible. Lorsque le premier mineur a trouvé la solution, il la fournit aux autres nœuds. La solution est ensuite vérifiée et un consensus est trouvé. Le mineur qui valide le nouveau bloc est récompensé par des bitcoins. Le degré de difficulté du problème mathématique augmente à mesure que les blocs sont minés pour faire en sorte qu'un seul bloc puisse être miné toutes les dix minutes (Kravisz, 2013).

Preuve d'enjeu (PoS – Nxt)

Les algorithmes de preuve d'enjeu sont destinés à surmonter l'inconvénient de la preuve de travail en termes de consommation d'énergie. La preuve d'enjeu remplace l'opération de minage par des récompenses proportionnelles au montant de la « participation » des validateurs dans le réseau (possession de cryptomonnaie ou actifs en cryptomonnaie dans le réseau). Cela améliore dans une certaine mesure la sécurité du réseau. La preuve d'enjeu est particulièrement utilisée par les organisations qui disposent d'une puissance de calcul limitée.

Preuve du temps écoulé (PoET – Hyperledger Sawtooth)

Utilisée par Hyperledger Sawtooth, la preuve du temps écoulé s'appuie sur un modèle de sélection aléatoire, ou de loterie, dans lequel le protocole sélectionne au hasard le prochain leader qui finalisera le bloc.

Algorithme pratique de tolérance aux fautes byzantines (PBFT – Hyperledger Iroha)*

Hyperledger Iroha, développé par la Fondation Linux, utilise un algorithme pratique de tolérance aux fautes byzantines. Dans ce système, chaque nœud distribue une clé publique et les messages sont signés par chaque nœud. Lorsqu'un nombre suffisant de réponses identiques a été obtenu, l'opération est considérée comme valide. Après l'algorithme pratique de tolérance aux fautes byzantines, plusieurs protocoles de tolérance aux fautes byzantines ont été développés pour améliorer la robustesse et la performance.

Accord fédéré byzantin (Ripple et Stellar)

Ripple et Stellar utilisent un processus de vote fédéré qui est une variante du modèle de consensus de tolérance aux fautes byzantines.

Note de fin

1. Le hachage présente diverses propriétés qui en font un outil intéressant pour assurer l'intégrité des données et empêcher leur falsification:

1. Un ensemble de données (entrée) donnera toujours le même hash (résultat). Cependant, un petit changement dans l'entrée – comme une simple modification des lettres ou de la ponctuation – modifiera complètement et radicalement le hash en résultant. Ce point est crucial pour la vérification de l'intégrité des données. Si une information produit des hashes différents pour l'expéditeur et le destinataire, cela signifie qu'elle a été manipulée pendant le transit. Si une donnée au repos change de hash entre le moment où elle est créée et celui où elle est vérifiée, cela indique qu'elle a fait l'objet de modifications dans l'intervalle. Cela permet donc utile de détecter immédiatement la falsification lorsqu'elle se produit.
2. Il est impossible de déterminer l'entrée initiale à partir de sa valeur de hachage. La probabilité de la «deviner» est très faible et nécessiterait une puissance de calcul considérable.
3. Un résultat et une entrée peuvent être comparés très rapidement, ce qui est très utile pour le traitement des gros fichiers de données et dans les cas nécessitant une certaine réactivité – par exemple dans les processus de vérification de l'identité de l'utilisateur, ou lorsqu'un utilisateur saisit son mot de passe pour accéder à un service, le système hache immédiatement le mot de passe saisi et le compare au hash enregistré.

4. Les fonctions de hachage sont dites « puzzle-friendly » : si un résultat est obtenu en combinant deux ensembles d'entrées, il est presque impossible d'identifier la valeur de l'un de ces ensembles même si l'on connaît déjà le second.
 5. Les fonctions de hachage sont « résistantes aux collisions » : la probabilité que deux entrées différentes donnent aléatoirement le même résultat est très faible, ce qui constitue un autre aspect contribuant à l'intégrité des données.
2. Dans le cas du protocole de preuve du travail utilisé, par exemple, par Bitcoin, on dit que le bloc est « miné ».
 3. Voir: <https://iota.readme.io/docs/what-is-iota>

Glossaire

Algorithmes à clés asymétriques

Il s'agit de l'un des deux types d'algorithmes utilisés pour le chiffrement.* Les algorithmes à clés asymétriques utilisent des clés différentes pour chiffrer et déchiffrer l'information. Ils relèvent de la catégorie de la cryptographie à clé publique. Ce type de chiffrement utilise deux clés qui fonctionnent par paires : une clé publique accessible à des tiers et une clé privée tenue secrète par le générateur de la paire. L'utilisation de clés différentes rend ce type de cryptographie plus commode à appliquer que la cryptographie à clé privée, mais elle augmente le risque d'attaques malveillantes. Pour atténuer ce risque, un niveau de sécurité supplémentaire est offert par l'introduction de certificats de sécurité, certificats numériques reliant une clé publique à une entité ou une personne particulière et délivrés par des autorités de certification de confiance.

Algorithmes à clés symétriques

Il s'agit de l'un des deux types d'algorithmes utilisés pour le chiffrement.* Les algorithmes à clés symétriques utilisent la même clé pour chiffrer et déchiffrer le texte. Ils font partie de ce qu'on appelle la cryptographie à clé privée.

Chaîne de blocs

Une chaîne de blocs est un recueil numérique de transactions (registre) horodaté et distribué, qui est sécurisé au moyen de diverses techniques cryptographiques. C'est une liste en constante augmentation d'entrées, ou de « blocs » « enchaînés » les uns aux autres au moyen d'outils de cryptographie. La chaîne de blocs est la technologie qui sous-tend le bitcoin. Les expressions « chaîne de blocs » et « technologie de registres distribués » sont souvent employées indifféremment. Mais, à proprement parler, la chaîne de blocs est un type de technologie de registres distribués.

Chiffrement

Le chiffrement est une technique cryptographique qui consiste à appliquer une fonction mathématique (souvent appelée algorithme) pour cacher une information ou la rendre secrète. Ce processus convertit des informations lisibles (texte en clair) en une séquence aléatoire illisible de caractères (texte chiffré). Le chiffrement est un processus bidirectionnel. Les données chiffrées peuvent être déchiffrées au moyen d'un code ou d'une clé. Le chiffrement contribue à la confidentialité des données car il protège les données en transit et au repos contre tout accès par des utilisateurs non autorisés en authentifiant les utilisateurs au moyen de clés. Cependant, comme le processus de chiffrement est intrinsèquement réversible, il ne suffit pas en soi pour garantir la sécurité de l'information, de sorte que les protocoles plus sûrs comme la chaîne de blocs utilisent le chiffrement combiné à d'autres techniques cryptographiques comme le hachage.

Le chiffrement consiste en deux types d'algorithmes : les algorithmes à clés symétriques* et les algorithmes à clés asymétriques.*

Code QR

Un code QR est un code qui est lisible par machine qui consiste en un pictogramme composé de carrés noirs et blancs et qui est généralement utilisé pour stocker des URL ou d'autres informations. Le code peut être lu avec la caméra d'un smartphone.

Contrat intelligent

Les contrats intelligents sont des programmes informatiques qui s'exécutent automatiquement lorsque certaines conditions sont remplies (selon la logique « si... alors... », par exemple, si les marchandises sont déchargées au port de X, alors les fonds seront transférés). Ils énoncent les obligations de chaque partie au « contrat », ainsi que les avantages et les pénalités pouvant s'appliquer à l'une ou l'autre des parties dans différentes circonstances.

Cryptographie

C'est un processus qui permet de communiquer de manière sûre dans un environnement peu sûr. La cryptographie est la science qui construit et analyse les protocoles utilisés pour assurer la sécurité de l'information, comme la confidentialité et l'intégrité des données et l'authentification. Ces éléments sont de plus en plus importants dans la communication moderne et ce sont des aspects essentiels des discussions qui se tiennent dans les instances de réglementation du commerce

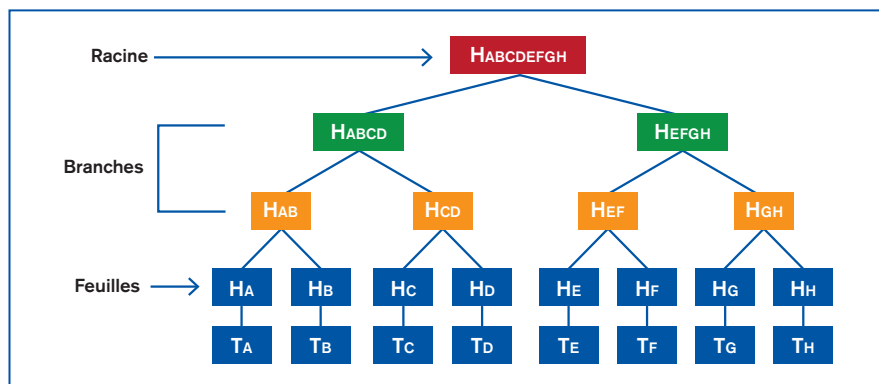
mondial – y compris l'OMC – au sujet du commerce électronique et de la dématérialisation des procédures commerciales transfrontalières.

Les termes «cryptographie» et «chiffrement» sont souvent utilisés de manière interchangeable. Cependant, le chiffrement n'est que l'une des techniques cryptographiques, avec le hachage et les signatures numériques.

Cryptomonnaie

Une cryptomonnaie est une monnaie numérique qui utilise la cryptographie à des fins de sécurité. La cryptomonnaie la plus connue est le bitcoin.

Diagramme d'un arbre de Merkle



Source : Auteure.

Notes : «T» désigne une transaction, et «H» un hash. Les blocs contiennent plusieurs centaines de transactions.

Ethereum

Ethereum est la deuxième chaîne de blocs publique après Bitcoin. Elle a fait un bond en avant avec le concept des contrats intelligents, programmes informatiques qui exécutent automatiquement les clauses d'un contrat lorsque certaines conditions sont remplies.

Faute byzantine

Des fautes ou des défaillances byzantines peuvent survenir en raison de bugs logiciels ou lorsqu'un nœud est compromis, ce qui entraîne un comportement

erratique des nœuds. Lamport *et al.* (1982) ont appelé ce type de défaillance «le problème des généraux byzantins» :

«Plusieurs généraux de l'armée byzantine campaient avec leurs troupes autour d'une ville ennemie. Ils ne peuvent communiquer entre eux qu'à l'aide de messagers et ils doivent se mettre d'accord sur un plan de bataille commun. Or il se peut qu'il y ait parmi eux un ou plusieurs traîtres, qui tenteront de semer la confusion parmi les autres. Le problème est donc de trouver un algorithme pour s'assurer que les généraux loyaux arriveront à se mettre d'accord. Il est démontré qu'en utilisant uniquement des messages oraux, ce problème peut être résolu si et seulement si plus des deux tiers des généraux sont loyaux; puisqu'un seul traître peut confondre deux généraux loyaux. Avec des messages écrits infalsifiables, le problème peut être résolu quel que soit le nombre de généraux et de traîtres potentiels» (Lamport *et al.*, 1982).

Hachage

Le hachage est une technique cryptographique qui consiste à appliquer une fonction mathématique (algorithme de hachage) pour convertir des données de taille arbitraire en une nouvelle chaîne numérique de longueur prédéfinie et fixe – un hash (voir l'exemple ci-dessous et Prpic, 2017).

Exemple de hachage

ENTRÉE	HASH
Hi	639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome	53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

Source: <https://blockgeeks.com/guides/what-is-hashing/>.

Le hachage a plusieurs propriétés qui en font un outil intéressant pour assurer l'intégrité des données et empêcher leur falsification :

- Un ensemble de données (entrée) donnera toujours le même hash (résultat). Ce point est important pour la vérification de l'intégrité des données. Si une information produit des hashes différents pour l'expéditeur et le destinataire, cela signifie qu'elle a été manipulée pendant le transit.
- Le hachage est souvent qualifié de «chiffrement unidirectionnel» car il est extrêmement difficile de déterminer l'entrée initiale à partir de sa valeur de hachage. La probabilité de la «deviner» est très faible et nécessiterait une puissance de calcul considérable.
- Les fonctions de hachage sont très efficaces: le calcul d'un résultat à partir d'une entrée est très rapide.

- Les fonctions de hachage sont dites «puzzle-friendly»: si un résultat est obtenu en combinant deux ensembles d'entrées (concaténées), il est presque impossible d'identifier la valeur de l'un de ces ensembles, même si le second est déjà connu.
- Les fonctions de hachage sont «résistantes aux collisions»: la probabilité que deux entrées différentes donnent aléatoirement le même résultat est extrêmement faible.

Horodatage

L'horodatage est l'opération consistant à utiliser des horodateurs numériques (données indiquant la date et l'heure) pour enregistrer la chronologie d'événements électroniques (par exemple, la création ou la modification d'un fichier de données, la soumission ou la réception d'une transaction, etc.). Chaque bloc d'une chaîne de blocs contient un horodateur unique.

L'horodatage est utilisé à des fins multiples, comme la sécurité informatique ou la gestion des réseaux et des bases de données, et comme preuve de l'exécution en temps voulu d'obligations entre des parties juridiquement liées (par un contrat) dans une transaction donnée. Il existe de nombreux protocoles d'horodatage; leur implémentation dépend du résultat souhaité.

Hyperledger Fabric

Hyperledger est une plate-forme libre née d'un effort de collaboration et destinée au développement de produits, de solutions et d'applications basés sur la chaîne de blocs pour les entreprises privées. Hébergé par la Fondation Linux, Hyperledger est un projet mondial qui réunit des leaders des secteurs de la finance, de la banque, de l'Internet des objets, des chaînes d'approvisionnement, de l'industrie et des technologies.

Logiciel libre

Un logiciel libre est un logiciel dont le code source peut être inspecté, modifié et amélioré par n'importe qui.

Minage

Le minage, dans le contexte de la technologie de la chaîne de blocs, est le processus par lequel les transactions sont vérifiées et ajoutées à une chaîne de blocs publique – la plus connue étant Bitcoin. C'est aussi le moyen par lequel de nouveaux bitcoins

sont émis. Le minage implique la résolution d'un puzzle mathématique compliqué. Le « mineur » qui est le premier à résoudre le puzzle peut ajouter un nouveau bloc à la chaîne de blocs et obtenir une récompense. Les récompenses, qui sont destinées à encourager le minage, comprennent à la fois les frais de transaction associés aux transactions contenues dans le bloc et les bitcoins nouvellement émis. Toute personne ayant des moyens appropriés (accès Internet et matériel adapté) peut pratiquer le minage.

Mineur

Personne qui pratique le minage (voir ci-dessus).

Monnaie fiduciaire

Une monnaie fiduciaire est une monnaie qu'un gouvernement a déclaré avoir cours légal, mais qui n'est pas adossée à un produit physique comme l'or ou l'argent.

Nœud

Un nœud est un ordinateur connecté au réseau. Chaque nœud conserve une copie des données ajoutées à la chaîne de blocs.

Nonce

Il s'agit d'une séquence de nombres aléatoire que les mineurs doivent trouver afin de valider le bloc d'une chaîne de blocs publique et la difficulté qui lui est associée. Les nonces font partie des éléments inclus dans les en-têtes de bloc des chaînes de blocs publiques.

Les blocs de chaînes de blocs privées n'ont pas de nonces.

Oracle

Les chaînes de blocs ne peuvent pas accéder aux données en dehors de leur réseau. Un oracle est un flux de données fourni par un prestataire de services tiers et destiné à être utilisé dans des contrats intelligents sur la chaîne de blocs. Il fournit des données externes et déclenche l'exécution de contrats intelligents lorsque des conditions prédéfinies sont remplies. Il peut s'agir de données telles que la température, l'exécution d'un paiement, les variations de prix, etc. Les oracles sont d'une importance cruciale car eux-seuls permettent aux contrats intelligents d'interagir avec les données en dehors de l'environnement de la chaîne de blocs.

Organisation autonome décentralisée (DAO)

Une organisation autonome décentralisée (DAO) est une organisation qui est gérée de façon autonome selon des règles définies dans des contrats intelligents. Pour plus de renseignements, voir : <https://blockchainhub.net/dao-decentralized-autonomous-organization/>.

Point de défaillance unique

Un élément ou une partie d'un système pouvant désactiver l'ensemble du système s'il tombe en panne.

Protocole de consensus

Il s'agit d'un protocole qui permet de valider les transactions et de signer les blocs dans la chaîne de blocs. Le protocole de consensus utilisé dépend du type de registre distribué et du niveau de confiance et de contrôle requis par l'application.

Les protocoles de consensus permettent de classer les transactions et les blocs de manière uniforme et claire, et garantissent l'intégrité et la cohérence de la chaîne de blocs entre des nœuds* répartis géographiquement.

Racine de Merkle et arbre de Merkle

La racine de Merkle est un élément de l'arbre de Merkle, une structure de données basée sur le hachage – ou arbre de hachage – qui est composée de feuilles et de branches, comme suit :

- Chaque feuille représente la valeur de hachage d'une transaction.
- Deux feuilles sont enchaînées («concaténées») et hachées pour former une branche.
- Ensuite, deux branches sont «concaténées» et hachées pour former une autre branche. Ce processus de hachage des branches se répète jusqu'à ce que le sommet de l'arbre – appelé «hash racine» – soit atteint.

En organisant les données selon cette structure, les arbres de Merkle rassemblent de grandes quantités de données et les rendent plus faciles à traiter. L'utilisation de la «racine de Merkle» dans l'en-tête d'un bloc permet de comparer et de vérifier facilement de grands ensembles de données de transactions sans avoir à inclure l'ensemble complet des données de chaque transaction dans l'en-tête de bloc, tout en fournissant un moyen de vérifier l'intégralité de la chaîne de blocs pour chaque transaction.

Pour comparer deux copies d'ensembles de données (qui peuvent être de très grande taille), il n'est donc pas nécessaire de vérifier tous les éléments de données des deux ensembles ; il suffit de vérifier la différence entre leurs deux arbres de hachage.

Par ailleurs, pour comparer deux arbres de hachage, il suffit de comparer les nœuds racines de ces arbres. Ce processus permet de vérifier beaucoup plus facilement et efficacement l'intégrité et la cohérence des données.

Si les deux nœuds racine comparés sont égaux, les données et leur ordre d'entrée dans l'arbre sont valides. Dans le cas contraire, si les arbres contiennent des données incohérentes, la structure ramifiée permet de rechercher plus aisément la source de l'incohérence. Pour déterminer l'origine de la différence entre deux arbres, il suffit de les parcourir de haut en bas pour trouver les nœuds puis les feuilles ayant des hachages différents.

La structure en arbre de Merkle réduit considérablement le temps nécessaire pour vérifier la cohérence et les données, et pour synchroniser les données dans les réseaux pair à pair et les registres distribués. Les systèmes de partage de fichiers, tels que Google Drive et Dropbox, sont deux applications qui utilisent les caractéristiques de l'arbre de Merkle : les changements sont détectés en comparant les nœuds racines, les nœuds branches et les nœuds feuilles, et seules les données qui doivent être synchronisées sont transférées de la source à la destination.

Registre distribué

Un registre distribué est un registre numérique – une liste, un tableur ou une base de données – qui est partagé entre les nœuds d'un réseau distribué. Les expressions « registre distribué » et « chaîne de blocs » sont souvent utilisées de manière interchangeable. Toutefois, à proprement parler, une chaîne de blocs n'est qu'un type de registre distribué.

Shard/Sharding

Le sharding désigne le fait de partitionner une très grande base de données en fragments plus petits, plus rapides et plus faciles à gérer, appelés shards. Le mot « shard » désigne une petite partie d'un tout.

Signature numérique

Une signature numérique est l'empreinte numérique d'un document électronique. Lorsque des données sont transmises entre un expéditeur et un destinataire, l'utilisation de signatures numériques garantit que le message a été créé et envoyé par l'expéditeur déclaré (authentification) et que le message n'a pas été modifié pendant le transit (intégrité des données). L'expéditeur ne peut pas nier avoir envoyé le message (non-répudiation).

Bibliographie

Accenture (2017), *Banking on Blockchain – A Value Analysis for Investment Banks*, Accenture, New York, Londres. Page consultée: «https://www.accenture.com/t20170120T074124Z__w_/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Consulting/Accenture-Banking-on-Blockchain.pdf», 20 janvier 2018.

Adegoke, Y. (2017), "Africa's Early Mobile Money Success is Finally Set to Go Global", *Quartz Africa*, 29 mai 2017. Page consultée: «<https://qz.com/993751/m-pesa-safaricom-kenya-regulators-and-vodacom-could-be-about-to-open-up-mobile-money-in-africa/>», 18 février 2018.

Alexandre, A. (2018), "Malta Passes Blockchain Bills Into Law, 'Confirming Malta as the Blockchain Island'", *Cointelegraph*, 5 juillet 2018. Page consultée: «https://cointelegraph.com/news/malta-passes-blockchain-blockchain-bills-into-law-confirming-malta-as-the-blockchain-blockchain-island?utm_source=newsletter1&utm_medium=email», 6 juillet 2018.

Allison, I. (2016), "Shipping giant Maersk tests blockchain-powered bill of lading", *International Business Times*, 14 octobre 2016. Page consultée: «<https://www.ibtimes.co.uk/shipping-giant-maersk-tests-blockchain-powered-bills-lading-1585929?webSyncID=6ccc1e6b-089a-2b6d-810d-e60990b22563&sessionGUID=8871313c-992a-4279-3293-95100716e18d>», 15 janvier 2018.

Allison, I. (2017a), "Axoni, Clearmatics Claim Milestone for Blockchain Interoperability", *Coindesk*, 17 mai 2018. Page consultée: «<https://www.coindesk.com/axoni-clearmatics-claim-milestone-business-blockchain-blockchain-interoperability/>», 15 janvier 2018.

Allison, I. (2017b), "Maersk and IBM want 10 million shipping containers on the global supply blockchain by year-end", *International Business Times*, 8 mars 2017. Page consultée: «<http://www.ibtimes.co.uk/maersk-ibm-aim-get-10-million-shipping-containers-onto-global-supply-blockchain-by-year-end-1609778>», 15 janvier 2018.

Androulaki, E. *et al.* (2018), «Hyperledger fabric: a distributed operating system for permissioned blockchains», compte rendu de la treizième conférence EuroSys, 23-26 avril 2018, Porto (Portugal). Page consultée: <https://dl.acm.org/citation.cfm?id=3190538>, 5 juin 2018.

Banque asiatique de développement (BASD) (2013), *E-Government Procurement Handbook*, BASD, Mandaluyong City (Philippines).

Banque asiatique de développement (BASD) (2017), *2017 Trade Finance Gaps, Growth, and Jobs Survey*, ADB Brief, n° 83, septembre 2017. Page consultée: «<https://www.adb.org/sites/default/files/publication/359631/adb-briefs-83.pdf>», 20 janvier 2018».

Banque mondiale (2017), *Doing Business 2017: Trading Across Borders – Technology gains in trade facilitation*, Banque mondiale, Washington (D.C.).

Barclays (2016), *The Blockchain Revolution in Trade Finance*, septembre 2016. Page consultée: «<https://www.barclayscorporate.com/insight-and-research/trading-and-exporting/blockchainBlockchain-revolution-in-trade-finance.html>», 22 novembre 2017.

Barry, C. et Zaccardi, P. (2015), *Cross-Border Payments: Challenges and Trends*, Aite Group Report. Page consultée: «<https://www.aitegroup.com/report/cross-border-payments-challenges-and-trends>», 15 janvier 2018.

Baydakova, A. (2018), "US Border Officials to Test Blockchain for Certificate Tracking", *Coindesk*, 17 août 2018. Page consultée: «<https://www.coindesk.com/us-border-officials-to-test-blockchain-for-tracking-import-certificates/>», 31 août 2018.

Bershidsky, L. (2017), "Bitcoin's High Transaction Fees Show its Limits", *Bloomberg*, 14 novembre 2017. Page consultée: «<https://www.bloomberg.com/view/articles/2017-11-14/bitcoin-s-high-transaction-fees-show-its-limits>», 18 janvier 2018.

Biryukov, A., Khovratovich, D., Pustogarov, I. (2014), "Deanonymisation of clients in Bitcoin P2P network", Université du Luxembourg, Working Paper, 5 juillet 2014. Page consultée: <https://arxiv.org/abs/1405.7418>, 20 janvier 2018.

BitFury Group (2015), «Public vs. Private Blockchains», White Paper, 20 octobre 2015. Page consultée: <https://bitfury.com/content/downloads/public-vs-private-pt1-1.pdf>, 18 janvier 2018.

Boston Consulting Group (2017), *Digital Innovation in Trade Finance: Have We Reached a Tipping Point?*, octobre 2017. Page consultée: «https://www.swift.com/news-events/news/digital-innovation-in-trade-finance-have-we-reached-a-tipping-point_», 10 novembre 2017.

Boucher, P. (2017), *Comment la technologie de la chaîne de blocs pourrait changer nos vies*, Service de recherche du Parlement européen, février 2017. Page consultée: «[http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA\(2017\)581948_FR.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_FR.pdf)», 17 octobre 2017.

Brady, D. (2017), "R3 Unveils Cross-Border Payments Platform Built on Corda DLT Tech", *Coindesk*, 31 octobre 2017. Page consultée: «<https://www.coindesk.com/r3-corda-international-payments/>», 22 novembre 2017.

Brandon, R. (2016), "How an Experimental Cryptocurrency lost (and found) \$53 million", *The Verge*, 17 juin 2016. Page consultée: «<https://www.theverge.com/2016/6/17/11965192/ethereum-theft-dao-cryptocurrency-million-stolen-bitcoin>», 21 octobre 2017.

Brown, R. G. (2016), "Introducing R3 Corda™: A Distributed Ledger Designed for Financial Services", *R3 Blog*, 5 avril 2016. Page consultée: «<http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services>», 22 novembre 2017.

Burstall, R. et Clark, B. (2017), "Blockchain, IP, and the fashion Industry", *Managing Intellectual Property*, 23 mars 2017. Page consultée: «<http://www.managingip.com/Article/3667444/Blockchain-IP-and-the-fashion-industry.html>», 16 janvier 2018.

Bustillos, M. (2013), "The Bitcoin Boom", *The New Yorker*, 1^{er} avril 2013. Page consultée: <https://www.newyorker.com/tech/elements/the-bitcoin-boom>, 10 octobre 2017.

Buterin, V. (2013), "Ethereum: The Ultimate Smart Contract and Decentralized Application Platform", Ethereum's White Paper. Page consultée: <http://web.archive.org/web/20131228111141/http://vbuterin.com/ethereum.html>, 8 janvier 2018.

Buterin, V. (2015), "On Public and Private Blockchains", *Ethereum blog*, 7 août 2015. Page consultée: «<https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchainblockchains/>», 8 janvier 2018.

Buterin, V. (2016), «Chain Interoperability», 9 septembre 2016. Page consultée: «<https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdf>», 13 avril 2018.

Buterin, V. (2018), «A Guide to 99% Fault Tolerant Consensus», 7 août 2018. Page consultée: «https://vitalik.ca/general/2018/08/07/99_fault_tolerant.html», 21 août 2018.

Cambridge Institute for Sustainability Leadership (CISL) (2017), "Blue chips and startups launch new fintech pilot for more sustainable supply chains at the One Planet Summit", 17 décembre 2017. Page consultée: «<https://www.cisl.cam.ac.uk/business-action/sustainable-finance/banking-environment-initiative/news/blue-chips-and-startups-launch-new-fintech-pilot>», 14 septembre 2018.

Campbell, R. (2016), "Babyghost and VeChain: Fashion on the Blockchain", *Nasdaq*, 18 octobre 2016. Page consultée: «<http://www.nasdaq.com/article/babyghost-and-vechain-fashion-on-the-blockchain-cm694925>», 5 mars 2018.

Carson, B., Romanelli, G., Walsh, P. et Zhumaev, A. (2018), "Blockchain beyond the hype: What is the strategic business value?", *McKinsey & Company*, juin 2018. Page consultée: «<https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value>», 2 juillet 2018.

Castell, H. (2018), "Blockchain in Trade: Are we Missing the Point?", *TXF News*, 8 janvier 2018. Page consultée: «<https://www.txfnews.com/News/Article/6338/Blockchain-in-trade-are-we-missing-the-point>», 9 janvier 2018 (accès limité aux membres).

Catalini, C. et Gans, J. (2017), "Some Simple Economics of the Blockchain", MIT Sloan Research Paper, n° 5191-16, 21 septembre 2017. Page consultée: «https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874598», 15 février 2018.

CB Insights (2017), "The March Of Financial Services Giants Into Bitcoin And Blockchain Startups In One Chart", Research Brief, 19 février 2017. Page consultée: «<https://www.cbinsights.com/research/financial-services-corporate-blockchain-investments/>», 20 janvier 2018.

CB Insights (2018), "Blockchain startups absorbed 5X more capital via ICOs than equity financings in 2017", 18 janvier 2018. Page consultée: «<https://www.cbinsights.com/research/blockchainBlockchain-vc-ico-funding/>», 20 janvier 2018.

CCN (2018), "Korea Customs Service to Pilot Blockchain-Based Import Customs Platform", 6 juin 2018. Page consultée: «<https://www.ccn.com/korea-customs-service-blockchainBlockchain-customs-clearance-platform/>», 20 juin 2018.

CEFACT/ONU (2018), "Blockchain White Paper: White Paper on the Technical Applications of Blockchain to CEFACT/ONU Deliverables", Draft White Paper, Projet au 30 avril 2018.

CEFACT/ONU (à paraître), *Trade, Facilitation and Financing – Building New Bridges in Trade-Based development*, CEFACT/ONU, Genève.

Cermeno, J. S. (2016), "Blockchain in financial services: regulatory landscape and future challenges for its commercial application", BBVA Research Paper, n° 16/20, décembre 2016. Page consultée: «https://www.bbvaresearch.com/wp-content/uploads/2016/12/WP_16-20.pdf», 20 janvier 2018.

Chambre de commerce internationale (ICC) (2017a), *2017 Rethinking Trade and Finance*, Paris, France: ICC, Paris.

Chambre de commerce internationale (ICC) (2017b), «ICC hails entry into force of WTO Trade Facilitation Agreement», ICC News, 22 février 2017. Page consultée: «<https://iccwbo.org/media-wall/news-speeches/icc-hails-entry-force-wto-trade-facilitation-agreement-watershed-moment-world-trade/>», 15 janvier 2018.

Chambre de commerce internationale (ICC) (2017c), «ICC Banking Commission launches working group on digitalisation of trade finance», ICC News, 6 juin 2017. Page consultée: «<https://iccwbo.org/media-wall/news-speeches/icc-banking-commission-launches-working-group-digitalisation-trade-finance/>», 15 janvier 2018.

Chaparro, F. (2017), «Bitcoin Miners are Making a Killing in Transaction Fees», *UK Business Insider*, 24 août 2017. Page consultée: «<http://uk.businessinsider.com/bitcoin-price-miners-making-killing-in-transaction-fees-2017-8?r=US&IR=T>», 18 janvier 2018.

Chohan, U. (2017), «Assessing the Differences in Bitcoin & Other Cryptocurrency Legality Across National Jurisdictions», University of New South Wales (UNSW) Business School, Working Paper, 20 septembre 2017. Page consultée: <https://ssrn.com/abstract=3042248>, 20 janvier 2018.

Choi, J. (2011), «A survey of single window implementation», OMD, Research Paper, n° 17, août 2011. Page consultée: «<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.696.1904&rep=rep1&type=pdf>», 14 janvier 2018.

Commission économique des Nations Unies pour l'Europe (CEE/ONU) (2017), *Summary of UNECE Trade Facilitation Recommendations*, Nations Unies, New York et Genève.

Commission économique et sociale des Nations Unies pour l'Asie et le Pacifique (CESAP/ONU) (2014), *Estimating the Benefits of Cross-Border Paperless Trade*, juin 2014, CESAP, Bangkok.

Commission économique et sociale des Nations Unies pour l'Asie et le Pacifique (CESAP/ONU) (2017), *Trade Facilitation and Paperless Trade Implementation – Global Report 2017*, Nations Unies, New York.

Commission européenne (2018), «La Commission européenne lance l'Observatoire-forum des chaînes de blocs de l'UE», Commission européenne – Communiqué de presse, 1^{er} février 2018. Page consultée: http://europa.eu/rapid/press-release_IP-18-521_fr.htm, 3 février 2018.

Commission européenne, (2004), *A Report on the Functioning of Public Procurement Markets in the EU: Benefits from the Application of EU Directives and Challenges for the Future*, Commission européenne, Bruxelles.

Conférence des Nations Unies sur le commerce et le développement (CNUCED) (2017), *Information Economy Report 2017: Digitalization, Trade and Development* (aperçu général en français: *Rapport sur l'économie de l'information 2017: numérisation, commerce et développement*), CNUCED, Genève.

Cong, L. W. (2018), «Blockchain Disruption and Smart Contracts», NBER Working Paper, mars 2018. Page consultée: <http://www.nber.org/papers/w24399>, 20 mai 2018.

Coppock, M. (2017), «The world's cryptocurrency mining uses more electricity than Iceland», *Digital Trends*, 7 juillet 2017. Page consultée: «<https://www.digitaltrends.com/computing/bitcoin-ethereum-mining-use-significant-electrical-power/>», 15 janvier 2018.

Corcuera-Santamaria, S. (2018), «Blockchain Platform to implement MRAs for AEO Programs», quatrième Conférence mondiale sur les OEA, Kampala (Ouganda), 14-16 mars 2018. Page consultée: [«https://www.eiseverywhere.com/file_uploads/5143a0f7208faa96709deb81df71f3a8_SandraCorcueraSantamaria_Blockchain-CADENAPresentation.pdf»](https://www.eiseverywhere.com/file_uploads/5143a0f7208faa96709deb81df71f3a8_SandraCorcueraSantamaria_Blockchain-CADENAPresentation.pdf), 10 septembre 2018.

Cory, N. (2017), *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, Information Technology and Innovation Foundation (ITIF) Report, 1^{er} mai 2017. Page consultée: [«https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost»](https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost), 20 janvier 2018.

Croman, K., Decker, C., Eyal, I., Gencer, E. A., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E. G., Song, D. et Wattenhofer, R. (2016), «On Scaling Decentralized Blockchains», Position Paper, 10 mars 2016. Page consultée: <https://www.tik.ee.ethz.ch/file/74bc987e6ab4a8478c04950616612f69/main.pdf>, 15 janvier 2018.

Darabi, A. (2018), «New Zealand Explores Machine-Readable Laws to Transform Government», *Apolitical*, 11 mai 2018. Page consultée: [«https://apolitical.co/solution_article/new-zealand-explores-machine-readable-laws-to-transform-government/»](https://apolitical.co/solution_article/new-zealand-explores-machine-readable-laws-to-transform-government/), 22 mai 2018.

De Filippi, P. et Hassan, S. (2018), «Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code», *First Monday* 21(12).

De, N. (2017), «Visa Launches First Phase of Blockchain B2B Payments», *Coindesk*, 17 novembre 2017. Page consultée: [«https://www.coindesk.com/visa-launches-first-phase-of-Blockchain-b2b-payments-system/»](https://www.coindesk.com/visa-launches-first-phase-of-Blockchain-b2b-payments-system/), 22 novembre 2017.

Decker, S. et Surrane, J. (2018), «BoFA Tops IBM, Payments Firms With Most Blockchain Patents», *Bloomberg Technology*, 16 janvier 2018. Page consultée: [«https://www.bloomberg.com/news/articles/2018-01-16/bofa-tops-ibm-and-payments-firms-with-most-blockchain-patents»](https://www.bloomberg.com/news/articles/2018-01-16/bofa-tops-ibm-and-payments-firms-with-most-blockchain-patents), 18 janvier 2018.

Del Castillo, M. (2017), «Consensus 2017: Blockchain Tech Leaders Predict Interoperable Future», *Coindesk*, 23 mai 2017. Page consultée: [«https://www.coindesk.com/consensus-2017-blockchainBlockchain-tech-leaders-predict-interoperable-future/»](https://www.coindesk.com/consensus-2017-blockchainBlockchain-tech-leaders-predict-interoperable-future/), 15 janvier 2018.

Del Castillo, M. (2018), «Shipping Blockchain: Maersk Spin-Off Aims to Commercialize Trade Platform», *Coindesk*, 16 janvier 2018. Page consultée: [«https://www.coindesk.com/shipping-blockchain-maersk-spin-off-aims-commercialize-trade-platform/»](https://www.coindesk.com/shipping-blockchain-maersk-spin-off-aims-commercialize-trade-platform/), 17 janvier 2018.

Delmolino, K., Arnett, M., Kosba, A., Miller, A., Shi, E. (2015), *Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab*, 18 novembre 2015. Page consultée: <https://eprint.iacr.org/2015/460.pdf>, 18 janvier 2018.

Deloitte (2016), *Blockchain in Insurance*. Page consultée: [«https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/financial-services/ca_en_financial_services_blockchain_in_insurance_AODA_new.PDF»](https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/financial-services/ca_en_financial_services_blockchain_in_insurance_AODA_new.PDF), 18 janvier 2018.

Deloitte (2017), *Blockchain & Cybersecurity*. Page consultée: [«https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf»](https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf), 2 février 2018.

Deloitte (2018), *Blockchain, legal implications, questions, opportunities and risks*, Deloitte Legal, mars 2018. Page consultée: «https://info.deloitte.com/rs/231-YWE-658/images/Blockchain%20WP%20March%202018_.pdf», 18 avril 2018.

eMarketer (2017), *Worldwide Retail and Ecommerce Sales: eMarketer's Estimates for 2016–2021*, eMarketer Report, 18 juillet 2017. Page consultée: «<https://www.emarketer.com/Report/Worldwide-Retail-Ecommerce-Sales-eMarketers-Estimates-20162021/2002090>», 15 novembre 2017.

Ernst&Young (2017), *Blockchain in insurance: applications and pursuing a path to adoption*. Page consultée: «[http://www.ey.com/Publication/vwLUAssets/EY-blockchain-in-insurance/\\$FILE/EY-blockchain-in-insurance.pdf](http://www.ey.com/Publication/vwLUAssets/EY-blockchain-in-insurance/$FILE/EY-blockchain-in-insurance.pdf)», 18 janvier 2018.

essDOCS (2018), "Introducing essCert – a next generation eCO solution", essDOCS News, 31 mai 2018. Page consultée: «<https://www.essdocs.com/blog/introducing-esscert-next-generation-eco-solution>», 20 juin 2018.

Ethereum White Paper. Page consultée: <https://github.com/ethereum/wiki/wiki/White-Paper>, 18 novembre 2017.

Financial Stability Board (FSB) (2018), *FSB Correspondent Banking Data Report*, 6 mars 2018. Page consultée: «<http://www.fsb.org/2018/03/fsb-correspondent-banking-data-report-update/>», 10 mars 2018.

Finck, M. (2017), "Blockchains and Data Protection in the European Union", Max Planck Institute for Innovation & Competition, Research Paper, n° 18-01, 30 novembre 2017. Page consultée: <https://ssrn.com/abstract=3080322>, 12 mars 2018.

Fonds monétaire internationale (FMI) (2017), "IMF Managing Director Welcomes Establishment of High Level Advisory Group on FinTech", FMI, communiqué de presse, 15 mars 2017. Page consultée: «<https://www.imf.org/en/News/Articles/2017/03/15/pr1784-imf-managing-director-welcomes-establishment-of-high-level-advisory-group-on-fintech>», 21 janvier 2018.

Fortune, A. (2016), "Philippines takes on meat import fraud through permit recall", *GlobalMeat News*, 23 novembre 2016. Page consultée: <https://www.globalmeatnews.com/Article/2016/11/23/Philippines-import-permit-recall>, 20 juin 2018.

Forum économique mondial (FEM) (2018), "Trade Tech – A New Age for Trade and Supply Chain Finance", White Paper in collaboration with Bain & Company, septembre 2018. Page consultée: <https://www.ibm.com/blogs/Blockchain/2018/01/digitizing-global-trade-maersk-ibm/>, 18 janvier 2018, 14 septembre 2018.

France24 (2018), "French art museum discovers more than half its collection is fake", version écrite en ligne, 30 avril 2018. Page consultée: «<http://www.france24.com/en/20180428-france-art-museum-etienne-terrus-fake-forgery>», 2 mai 2018.

Friedman, S. (2017), "GSA looks to blockchain for speeding procurement processes", *GCN*, 21 septembre 2017. Page consultée: <https://gcn.com/articles/2017/09/21/gsa-looks-to-blockchain-for-procurement.aspx>, 21 février 2018.

Gabison G. (2016), "Policy Considerations for the Blockchain Technology Public and Private Applications", *SMU Science & Technology Law Review*, volume 19. Page consultée: <http://scholar.smu.edu/scitech/vol19/iss3/4>, 10 mars 2018.

Gartner (2018), *Blockchain-Based Transformation: A Gartner Trend Insights Report*, 27 mars 2018, Gartner, Stamford (Connecticut). Page consultée: <https://www.gartner.com/doc/3869696?ref=unauthreader&srcId=1-4730952011>, 11 avril 2018.

Giles, F. (2018), "Is Blockchain the Future of Food Safety?", *Growing Produce*, 17 août 2018. Page consultée: <https://www.growingproduce.com/fruits/blockchain-future-food-safety/>, 21 août 2018.

Groenfeldt, T. (2017), "7 European Banks Form Blockchain Consortium For SMEs", *Forbes*, 28 juin 2017. Page consultée: <https://www.forbes.com/sites/tomgroenfeldt/2017/06/28/7-european-banks-form-blockchain-consortium-for-smes/#60ad78aa3818>, 22 novembre 2017.

Gronholt-Pedersen, J. (2018), "Maersk, IBM to launch blockchain-based platform for global trade", *Reuters*, 16 janvier 2018. Page consultée: <https://uk.reuters.com/article/uk-maersk-blockchain-ibm/maersk-ibm-to-launch-blockchain-based-platform-for-global-trade-idUKKBN1F51D5>, 17 janvier 2018.

Haber, S. et Stornetta, W. S. (1991), "How to time-stamp a digital document", *Journal of Cryptology*, 3 (2), pages 99 à 111.

Hackett, R. (2017), "Walmart and 9 Food Giants Team Up on IBM Blockchain Plans", *Fortune Magazine*, 22 août 2017. Page consultée: <http://fortune.com/2017/08/22/walmart-blockchain-ibm-food-nestle-unilever-tyson-dole/>, 15 janvier 2018.

Heap, I. (2017), "Blockchain Could Help Musicians Make Money Again", *Harvard Business Review*, 5 juin 2017. Page consultée: <https://hbr.org/2017/06/blockchain-could-help-musicians-make-money-again>, 10 janvier 2018.

Higgins, S. (2017a), "New Alliance Sets Out to Boost Blockchain Interoperability", *Coindesk*, 28 novembre 2017. Page consultée: <https://www.coindesk.com/new-alliance-sets-out-to-boost-blockchainBlockchain-interoperability/>, 21 janvier 2018.

Higgins, S. (2017b), "Spotify Acquires Blockchain Startup Mediachain", *Coindesk*, 26 avril 2017. Page consultée: <https://www.coindesk.com/spotify-acquires-blockchainBlockchain-startup-mediachain/>, 15 janvier 2018.

Higgins, S. (2017c), "Walmart: Blockchain Food Tracking Test Results Are 'Very Encouraging'", *Coindesk*, 5 juin 2017. Page consultée: <https://www.coindesk.com/walmart-blockchain-food-tracking-test-results-encouraging/>, 15 janvier 2018.

Higgins, S. (2018), "Enterprise Ethereum Alliance Unveils Common Blockchain Standards", *Coindesk*, 16 mai 2018. Page consultée: <https://www.coindesk.com/enterprise-ethereum-alliance-unveils-common-blockchain-standards/>, 17 mai 2018.

Hilbert, M. (2016), "The bad news is that the digital access divide is here to stay: Domestically installed bandwidths among 172 countries for 1986–2014", *Telecommunications Policy*, volume 40, n° 6, pages 567 à 581.

Hofmann, E., Strewé, U. M. et Bosia, N. (2017), *Supply Chain Finance and Blockchain Technology: The Case of Reverse Securitisation*, Springer.

HSBC (2016), "BofAML, HSBC, IDA Singapore Build Pioneering Blockchain Trade Finance App", HSBC Press Release, 10 août 2016. Page consultée: <http://www.about.hsbc.com.sg/-/media/singapore/en/press-releases/160810-blockchainBlockchain-letter-of-credit.pdf>, 22 novembre 2017.

Huertas, J., Liu, H. et Robinson, S. (2018), « Eximchain: Supply Chain Finance solutions on a secured public, permissioned blockchain hybrid », Eximchain White Paper, 13 mars 2018. Page consultée: «<https://eximchain.com/Whitepaper%20-%20Eximchain.pdf>», 28 mai 2018.

Huillet, M. (2018a), « China: Central Bank's Blockchain Trade Finance Platform Pilots in Shenzhen », *Cointelegraph*, 12 septembre 2018. Page consultée: «<https://cointelegraph.com/news/chinas-central-bank-backed-blockchain-trade-finance-platform-pilot-kicks-off-in-shenzhen>», 17 septembre 2018.

Huillet, M. (2018b), « China's Supreme Court Rules That Blockchain Can Legally Authenticate Evidence », *Cointelegraph*, 7 septembre 2018. Page consultée: «<https://cointelegraph.com/news/chinas-supreme-court-rules-that-blockchain-can-legally-authenticate-evidence>», 16 septembre 2018.

IBM (2016), « IBM to Open Blockchain Innovation Center in Singapore to Accelerate Blockchain Adoption for Finance and Trade », IBM News Release, 11 juillet 2016. Page consultée: <http://www-03.ibm.com/press/us/en/pressrelease/50163.wss>, 10 octobre 2017.

IBM (2017), « AIG, IBM, Standard Chartered Deliver First Multinational Insurance Policy Powered by Blockchain », IBM News Release, 15 juin 2017. Page consultée: <http://www-03.ibm.com/press/us/en/pressrelease/52607.wss>, 15 janvier 2018.

IBM (2018), « Blockchain and GDPR », White Paper, mars 2018. Page consultée: <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=61014461USEN>, 16 avril 2018.

Investoo Group (2017), « History of Ethereum: How it's set to overtake Bitcoin by 2018 », 26 juin 2017. Page consultée: «<http://www.mining.com/web/history-ethereum-set-overtake-bitcoin-2018/>», 21 octobre 2017.

IT News Africa (2018), « World's first blockchain-based e-Certificate of Origin unveiled in Singapore », 9 mai 2018. Page consultée: «<http://www.itnewsafrika.com/2018/05/worlds-first-blockchain-based-e-certificate-of-origin-unveiled-in-singapore/>», 20 juin 2018.

J.P. Morgan (2017), « J.P. Morgan Deploys Blockchain With New Correspondent Banking Network », J.P. Morgan News, 16 octobre 2017. Page consultée: <https://www.jpmorgan.com/country/FR/en/detail/1320562088910>, 22 novembre 2017.

Kelly, J. (2017), « EY teams up with Maersk, Microsoft on blockchain-based marine insurance », *Reuters*, 6 septembre 2017. Page consultée: «<https://www.reuters.com/article/us-blockchain-insurance-marine/ey-teams-up-with-maersk-microsoft-on-blockchain-based-marine-insurance-idUSKCN1BG3B6>», 15 janvier 2018.

KPMG (2017), *The Promise of Blockchain in Insurance*, 7 septembre 2017. Page consultée: «<https://home.kpmg.com/xx/en/home/insights/2017/09/the-promise-of-blockchain-in-insurance.html>», 15 janvier 2018.

Kravisz, D. (2013), *The Proof-of-Work Concept*, Satoshi Nakamoto Institute, 24 juin 2013. Page consultée: «<http://nakamotoinstitute.org/mempool/the-proof-of-work-concept/#select-ion-127.198-127.306>», 21 octobre 2017, 11 octobre 2017.

Lamport, L., Shostak, R. et Pease, M. (1982), « The Byzantine Generals Problem », *ACM Transactions on Programming Languages and Systems*, volume 4, n° 3, juillet 1982.

Lehmacher, W. (2017), *Why blockchain should be global trade's next port of call*, Forum économique mondial, 23 mai 2017, FEM, Genève. Page consultée: <https://www.weforum.org/agenda/2017/05/blockchain-ports-global-trades/>, 15 janvier 2018.

Leising, M. et Robinson, E. (2018), "Ripple Wants XRP to Be Bitcoin for Banks. If Only the Banks Wanted It", *Bloomberg BusinessWeek*, 25 janvier 2018. Page consultée: <https://www.bloomberg.com/news/articles/2018-01-25/ripple-wants-xrp-to-be-bitcoin-for-banks-if-only-the-banks-wanted-it>, 26 janvier 2018.

Lessig, L. (1999), *Code and Other Laws of Cyberspace*, volume 3, Basic books, New York.

Lewis, A. (2015), "A Gentle Introduction to Blockchain Technology", 9 septembre 2015. Page consultée: <https://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-Blockchain-technology/>, 6 février 2018.

Logistics and Fintech News (2017), "Wave One Step Closer to Blockchain-Based Solution for Paperless Trade", 24 novembre 2017. Page consultée: <http://logisticsandfintech.com/wave-one-step-closer-blockchainBlockchain-based-solution-paperless-trade/>, 25 novembre 2017.

Lohade, N. (2017), "Dubai Aims to Be a City Built on Blockchain", *The Wall Street Journal*, 24 avril 2017. Page consultée: <https://www.wsj.com/articles/dubai-aims-to-be-a-city-built-on-blockchain-1493086080>, 12 janvier 2018.

Lomas, N. (2016), "Circle Takes \$60M to Grow its Social Payments Biz Globally, as it Steps into China", *Techcrunch*, 23 juin 2016. Page consultée: <https://techcrunch.com/2016/06/22/circle-takes-60m-to-grow-its-social-payments-biz-globally-as-it-steps-into-china/>, 2 février 2018.

Manders, S. (2018), "Swift finds blockchain 'has potential' but will not commit yet", *Global Trade Review (GTR)*, 19 octobre 2017. Page consultée: <https://www.gtreview.com/news/fintech/swift-finds-blockchain-has-potential-but-will-not-commit-yet/>, 8 mars 2018.

Marine Transport International (MTI) (2017), "Blockchain System Successfully Deployed to Revolutionise the Logistics Industry", MTI News, 30 août 2017. Page consultée: <https://www.prnewswire.com/news-releases/blockchain-system-successfully-deployed-to-revolutionise-the-logistics-industry-642213333.html#>, 8 mai 2018.

Marshall, A. (2017), "What the Fork? New SegWit2x Launches With Massive Premine, Unknown Development Team", *Cointelegraph*, 29 décembre 2017. Page consultée: <https://cointelegraph.com/news/what-the-fork-new-segwit2x-launches-with-massive-premine-unknown-development-team>, 15 janvier 2018.

Mastercard (2017), "Mastercard Opens-Up Access to Blockchain API for Partner Banks and Merchants", communiqué de presse, 20 octobre 2017. Page consultée: <https://newsroom.mastercard.com/press-releases/mastercard-opens-access-Blockchain-api-partner-banks-merchants/>, 22 novembre 2017.

Mbogo, A. (2018), "Africa to Adopt Blockchain for New Digital Free Trade Area", *Bitcoin Africa*, 28 février 2018. Page consultée: <http://bitcoinafrica.io/2018/02/28/africa-to-adopt-blockchain-for-new-digital-free-trade-area/>, 20 juin 2018.

McKinsey & Company (2016a), *Blockchain in insurance—opportunity or threat?*, juillet 2016. Page consultée: <https://www.mckinsey.com/industries/financial-services/our-insights/blockchain-in-insurance-opportunity-or-threat>, 15 janvier 2018.

McKinsey & Company (2016b), *Global Payments: Strong Fundamentals Despite Uncertain Times*, septembre 2016. Page consultée: «<https://www.mckinsey.com/~media/McKinsey/Industries/Financial%20Services/Our%20Insights/A%20mixed%202015%20for%20the%20global%20payments%20industry/Global-Payments-2016.ashx>», 15 janvier 2018.

McKinsey & Company (2016c), "Rethinking Correspondent Banking", *McKinsey on Payments*, volume 9, n° 23, juin 2016.

McKinsey & Company (2017), "Blockchain Technology in the Insurance Sector", Quarterly meeting of the Federal Advisory Committee on Insurance (FACI), 5 janvier 2017. Page consultée: «https://www.treasury.gov/initiatives/fio/Documents/McKinsey_FACI_Blockchain_in_Insurance.pdf», 15 janvier 2018.

Mearian, L. (2017), "FinTech builds on blockchain for international mobile payments", *ComputerWorld*, 15 octobre 2017. Page consultée: «<https://www.computerworld.com/article/3233187/mobile-wireless/fintech-builds-on-blockchain-for-international-mobile-payments.html>», 2 février 2018.

Mertens, E. (2018a), "How Blockchain will change Intellectual Property – Patents", 6 mars 2018, *Managing Intellectual Property*. Page consultée: www.managingip.com, 10 mars 2018.

Mertens, E. (2018b), "How Blockchain will change Intellectual Property – Trademarks and Brands", 27 février 2018, *Managing Intellectual Property*. Page consultée: www.managingip.com, 10 mars 2018.

Millward, S. (2017), "Alibaba to use blockchain to fight China's fake food", *TechInAsia*, 24 mars 2017. Page consultée: «<https://www.techinasia.com/alibaba-fake-food-detection-blockchain>», 15 janvier 2018.

Monteleone, L. (2018), "How Blockchain will alter Trademarks' registration and enforcement?", *Media Laws*, 8 mars 2018. Page consultée: «<http://www.medialaws.eu/how-blockchain-will-alter-trademarks-registration-and-enforcement/>», 10 mars 2018.

Naden, C. (2017), "L'essor de la technologie de la chaîne de blocs porté par la normalisation internationale", *ISO News*, 24 mai 2017. Page consultée: <https://www.iso.org/fr/news/Ref2188.htm>, 15 janvier 2018.

Nakamoto, S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*. Page consultée: <https://bitcoin.org/bitcoin.pdf>, 10 octobre 2017.

Nasdaq (2015), «Nasdaq Linq Enables First-Ever Private Securities Issuance Documented With Blockchain Technology», communiqué de presse, 30 décembre 2015. Page consultée: <http://ir.nasdaq.com/releasedetail.cfm?releaseid=948326>, 12 février 2018.

Noonan, L. (2018), "China leads blockchain patent applications", *The Financial Times*, 25 mars 2018.

OCDE-EU IPO (2016), *Trade in Counterfeit and Pirated Goods* (résumé analytique en français: *Le commerce des produits contrefaisants et piratés*), 18 avril 2016.

O'Dwyer, K. et Malone, D. (2014), "Bitcoin Mining and its Energy Footprint", National University of Ireland Maynooth, Working Paper, 26 juin 2014. Page consultée: http://karlodwyer.com/publications/pdf/bitcoin_KJOD_2014.pdf, 10 mars 2018.

Ohnesorge, J. (2018), "A Primer on Blockchain Technology and Its Potential for Financial Inclusion", German Development Institute, Discussion Paper, 2/2018, German Development Institute, Bonn.

OMC (2016b), *Le financement du commerce et les PME – Comblant les lacunes en matière d'offre*, OMC, Genève.

Orcutt, M. (2018), "States that are passing laws to govern "smart contracts" have no idea what they're doing", *MIT Technology Review*, 29 mars 2018. Page consultée: «<https://www.technologyreview.com/s/610718/states-that-are-passing-laws-to-govern-smart-contracts-have-no-idea-what-theyre-doing/>», 20 janvier 2018.

Organisation de coopération et de développement économiques (OCDE) (2016), *Prévention de la corruption dans les marchés publics*, OCDE, Paris.

Organisation de coopération et de développement économiques (OCDE) (2017), «Renforcer les contributions des PME dans une économie mondialisée et numérique», compte rendu de la réunion du Conseil de l'OCDE au niveau des Ministres, 7-8 juin 2017, OCDE, Paris.

Organisation mondiale de la santé (2016), *Counterfeit Medicines: an update on estimates*, 15 novembre 2016, OMS, Genève.

Organisation mondiale des douanes (OMD) (2017), «Blockchains», *Information Management Sub-Committee*, soixante-douzième réunion, 19 avril 2017, OMD, Bruxelles.

Organisation mondiale du commerce (OMC) (2015a), *Commerce et droits de douane*, OMC, Genève.

Organisation mondiale du commerce (OMC) (2015b), *Commerce des services – Le segment le plus dynamique du commerce international*, OMC, Genève.

Organisation mondiale du commerce (OMC) (2015c), *Rapport sur le commerce mondial 2015 – Accélérer le commerce: avantages et défis de la mise en œuvre de l'Accord de l'OMC sur la facilitation des échanges*, OMC, Genève.

Organisation mondiale du commerce (OMC) (2016a), «Commerce électronique et droit d'auteur», communication présentée par le Brésil, document JOB/GC/113, 15 décembre 2016, OMC, Genève.

Palfreman, L. (2017), "Blockchain or blocked chain?", *TXF News*, 23 août 2017. Page consultée: «<https://www.txfnews.com/News/Article/6200/Blockchain-or-blocked-chain>», 10 octobre 2017.

Park, T. (2018), "Blockchain Is About to Revolutionize the Shipping Industry", *Bloomberg*, 18 avril 2018. Page consultée: «<https://www.bloomberg.com/news/articles/2018-04-18/drowning-in-a-sea-of-paper-world-s-biggest-ships-seek-a-way-out>», 20 avril 2018.

Parker, L. (2017), "US States working on blockchain legislation", *BraveNewsCoin*, 2 avril 2017. Page consultée: «<https://bravenewcoin.com/news/us-states-working-on-blockchain-legislation-in-2017/>», 15 janvier 2018.

Parlement européen (2018), «Projet de rapport sur la chaîne de blocs: une politique commerciale tournée vers l'avenir», Projet de rapport 2018/2085, daté du 18 juillet 2018, Commission du commerce international.

Perez, B. (2017), "Hong Kong's monetary authority unveils trade finance platform based on blockchain technology", *TheStreet*, 30 mars 2017. Page consultée: «<https://www.thestreet.com/story/14065398/1/hong-kongs-monetary-authority-unveils-trade-finance-platform-based-on-bitcoin-tech.html>», 10 octobre 2017.

Persio, S. L. (2016), "Banks bring blockchain innovation to letters of credit", *Global Trade Review*, 10 août 2016. Page consultée: «<https://www.gtreview.com/news/asia/banks-blockchain-innovation-letters-of-credit/>», 10 janvier 2018.

PriceWaterHouseCoopers (2016), *Chain Reaction: How Blockchain Technology Might Transform Wholesale Insurance*, juillet 2016. Page consultée: «<https://www.pwc.com/gx/en/industries/financial-services/publications/blockchain-technology-might-transform-wholesale-insurance.html>», 15 janvier 2018.

Prpic, J. (2017), «Unpacking Blockchains», *Collective Intelligence* 2017. Page consultée: <https://arxiv.org/ftp/arxiv/papers/1703/1703.06117.pdf>, 10 janvier 2018.

R3 and Norton Rose Fulbright (2017), "Can smart contracts be legally binding contracts", R3 and Norton Rose Fulbright White Paper, novembre 2016. Page consultée: «<https://www.natlawreview.com/article/blockchain-and-virtual-currency-regulation-eu>», 20 janvier 2018.

Ralph, O. (2017), "AIG sets up blockchain policy for Standard Chartered", *The Financial Times*, 15 juin 2017. Page consultée: <https://www.ft.com/content/03ea1b88-511b-11e7-a1f2-db19572361bb>, 15 janvier 2018.

Rapport sur le commerce mondial (OMC) (2016c), *Rapport sur le commerce mondial 2016: Égaliser les conditions du commerce pour les PME*, OMC, Genève.

Redman, J. (2017), "Rising Network Fees Are Causing Changes Within the Bitcoin Community", *BitcoinNews*, 9 juin 2017. Page consultée: <https://news.bitcoin.com/fees-causing-changes-bitcoin-economy/>, 18 janvier 2018.

Roubini, N. et Preston, B. (2018), «The Blockchain Pipe Dream», *Project Syndicate*, version en ligne, 5 mars 2018. Page consultée: «<https://www.project-syndicate.org/commentary/blockchain-technology-limited-applications-by-nouriel-roubini-and-preston-byrne-2018-03?barrier=accesspaylog>», 7 mars 2018.

Santander, InnoVentures, Oliver Wyman, and Anthemis Group (2015), *The Fintech 2.0 Paper: rebooting financial services*, juin 2015. Page consultée: «<https://www.finextra.com/finextra-downloads/newsdocs/the%20fintech%202%200%20paper.pdf>», 15 janvier 2018.

Savelyev A. (2017), "Copyright in the Blockchain Era", National Research University, Higher School of Economics, Working Paper Basic Research Program, 77/LAW/2017.

Service d'information des Nations Unies (SINU) (2017), «UN Commission on International Trade Law adopts the UNCITRAL Model Law on Electronic Transferable Records», SINU, communiqué de presse, 17 juillet 2017, Page consultée: <http://www.unis.unvienna.org/unis/en/pressrels/2017/unis1251.html>, 15 janvier 2018.

Siegel, D. (2016), "Understanding the DAO Attack", *Coindesk*, 25 juin 2016. Page consultée: <https://www.coindesk.com/understanding-dao-hack-journalists/>, 21 octobre 2017.

Skinner, C. (2016), "Will the Blockchain Replace SWIFT", *American Banker*, 8 mars 2016. Page consultée: <https://www.americanbanker.com/opinion/will-the-blockchain-replace-swift>, 15 janvier 2018.

Smirke, R. (2017), "ASCAP, SACEM and PRS For Music Team Up on Initiative to Improve Royalty Collection", *BillBoard*, 4 juillet 2017. Page consultée: «<http://www.billboard.com/articles/business/7752442/ascap-sacem-prs-for-music-initiative-improve-royalty-collection>», 15 janvier 2018.

Société financière internationale (SFI) (2017), *Blockchain Opportunities for Private Enterprises in Emerging Markets*, octobre 2017, SFI, Washington (D.C.), IFC.

Stokes, P. (2017), "Electronic Sanitary and Phytosanitary Certificates in the Context of Paperless Trade", Background Paper, mai 2017.

Suberg, W. (2018), "IBM-Powered Blockchain Platform Completes First Live Trades Via Five Major Banks", *Cointelegraph*, 3 juillet 2018. Page consultée: «https://cointelegraph.com/news/ibm-powered-blockchain-platform-completes-first-live-trades-via-five-major-banks?utm_source=newsletter1&utm_medium=email», 4 juillet 2018.

Sullivan, C. et Burger, E. (2017), "E-Residency and Blockchain", *Computer Law & Security Review*, volume 33, n° 4, pages 470 à 481.

SWIFT (2018a), *Blockchain: gpi Nostro Proof of Concept – final report*, mars 2018.

SWIFT (2018b), "SWIFT completes landmark DLT PoC", SWIFT Press Release, 8 mars 2018. Page consultée: «<https://www.swift.com/news-events/press-releases/swift-completes-landmark-dlt-poc>», 8 mars 2018.

Takahashi, K. (2017), "Implications of the Blockchain Technology for the UNCITRAL Works", Working Paper, 15 juin 2017. Page consultée: «<https://onedrive.live.com/?authkey=pourcent21AMLDDJc03VocQms&cid=431D6C57123F90CF&id=431D6C57123F90CFpourcent212163&parld=root&o=OneUp>», 15 janvier 2018.

Takahashi, K. (2018), "Blockchain Technology for Letters of Credit and Escrow Arrangements", *The Banking Law Journal*, février 2018, New York: LexisNexis.

Tapscott, D. et Tapscott, A. (2017), "Realizing the Potential of Blockchain", Forum économique mondial (FEM), White Paper, juin 2017. Page consultée: http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf, 10 janvier 2018.

Tapscott, D. et Tapscott, A. (2018), *Blockchain Revolution: How the Technology Behind Bitcoin and other cryptocurrencies is Changing the World*, Portfolio Penguin, Londres.

The Economist (2015), "The Trust Machine – The Promise of the Blockchain", 31 octobre 2015. Page consultée: «<https://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine>», 18 novembre 2017.

The Maritime Executive (2018), «APL Tests Blockchain Solution», 17 mars 2018. Page consultée: «<https://www.maritime-executive.com/article/apl-tests-blockchain-solution#gs.Dh8PQvU>», 19 mars 2018.

Tian, C. (2017), "Japan to Test Blockchain for Government Contract System", *Coindesk*, 30 juin 2017. Page consultée: «<https://www.coindesk.com/japan-test-blockchain-government-contract-system/>», 21 février 2018.

Toth, A. (2018), "Will GDPR Block Blockchain", World Economic Forum, 24 mai 2018. Page consultée: «<https://www.weforum.org/agenda/2018/05/will-gdpr-block-blockchain/>», 25 mai 2018.

T'Serclaes, P. (2017), "Blockchain could be the missing link in the renewable energy revolution", Forum économique mondial, 21 septembre 2017. Page consultée: <https://www.weforum.org/agenda/2017/09/blockchain-energy-efficiency-finance/>, 15 janvier 2018.

UNNExT, CEE/ONU, CESAP/ONU (2012), *Electronic Single Window Legal Issues: A Capacity Building Guide*, publication des Nations Unies.

Vogel N. (2015), "The Great Decentralization: How Web 3.0 Will Weaken Copyrights", 15 *J. Marshall Rev. Intell.Prop. L.* 136 (2015).

Wass, S. (2018a), "IBM's latest blockchain venture brings microfinancing to Africa's SMEs", *Global Trade Review*, 18 avril 2018. Page consultée: <https://www.gtreview.com/news/fintech/ibms-latest-blockchain-venture-brings-microfinancing-to-africas-smes/>, 18 mai 2018.

Wass, S. (2018b), "Maersk and IBM go live with global blockchain trade platform TradeLens", *Global Trade Review*, 18 août 2018. Page consultée: <https://www.gtreview.com/news/fintech/maersk-and-ibm-go-live-with-blockchain-supply-chain-platform-tradelens/>, 19 août 2018.

Weinland, D. (2018), "HSBC Claims First Trade-Finance Deal with Blockchain", *Financial Times*, 13 mai 2018. Page consultée: <https://www.ft.com/content/c0670eb6-5655-11e8-bdb7-f6677d2e1ce8>, 14 mai 2018.

Werbach K. (2018), "Trust, But Verify: Why the Blockchain Needs the Law", *Berkeley Technology Law Journal*, à paraître. Page consultée: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2844409, 30 juin 2018.

White, M. (2018), "Digitizing Global Trade with Maersk and IBM", *IBM Blockchain Blog*, 16 janvier 2018. Page consultée: <https://www.ibm.com/blogs/Blockchain/2018/01/digitizing-global-trade-maersk-ibm/>, 18 janvier 2018.

Abréviations

\$EU	dollars des États-Unis
ADPIC	Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce
AFE	Accord sur la facilitation des échanges
AGCS	Accord général sur le commerce des services
AMP	Accord sur les marchés publics
API	interface de programmation d'applications
ARM	accord de reconnaissance mutuelle
ASEAN	Association des nations de l'Asie du Sud-Est
BAD	Banque asiatique de développement
ITC	Centre du commerce international
ICC	Chambre de commerce internationale
CEFACT-ONU	Centre des Nations Unies pour la facilitation du commerce et les transactions électroniques
CESAP	Commission économique et sociale pour l'Asie et le Pacifique
CIPV	Convention internationale pour la protection des végétaux
CITES	Convention sur le commerce international des espèces de faune et de flore sauvages menacées d'extinction
CNUCED	Conférence des Nations Unies sur le commerce et le développement
code QR	code Quick Response
DAO	organisation autonome décentralisée
EUIPO	Office de l'Union européenne pour la propriété intellectuelle
EUR	euros
FANDC	Fonds pour l'application des normes et le développement du commerce
FAO	Organisation des Nations Unies pour l'alimentation et l'agriculture
FSB	Conseil de stabilité financière

GATT	Accord général sur les tarifs douaniers et le commerce
ISO	Organisation internationale de normalisation
kWh	kilowattheures
MPME	micro, petites et moyennes entreprises
OCDE	Organisation de coopération et de développement économiques
OEA	opérateur économique agréé
OIE	Organisation mondiale de la santé animale
OMC	Organisation mondiale du commerce
OMD	Organisation mondiale des douanes
OMPI	Organisation mondiale de la propriété intellectuelle
OMS	Organisation mondiale de la Santé
PIB	produit intérieur brut
PMA	pays les moins avancés
RGPD	Règlement général sur la protection des données de l'Union européenne
SWIFT	Société de télécommunications interbancaires mondiales
SYDONIA	Système douanier automatisé de la CNUCED
TI	technologie de l'information
UE	Union européenne
UIT	Union internationale des télécommunications
USITC	Commission du commerce international des États-Unis

Liste des graphiques et tableaux

Figures

Figure 1	Registre centralisé et registre distribué	6
Figure 2	Le degré de décentralisation des registres distribués varie	11
Figure 3	Documents types émis dans le cadre du commerce international	20
Figure 4	Quatre processus intervenant dans les transactions commerciales transfrontières	21
Figure 5	Utilisation de lettres de crédit ou compte ouvert (volume des échanges mondiaux de 1978 à 2013)	22
Figure 6	Le processus traditionnel de financement du commerce est très fragmenté entre de multiples entités et processus	23
Figure 7	De nombreux acteurs, documents et éléments de données interviennent dans une transaction de financement du commerce	24
Figure 8	Exemple de processus de lettre de crédit	26
Figure 9	Scénarios des processus G2G transfrontières	43
Figure 10	Projet de numérisation du commerce mondial Maersk-IBM	49
Figure 11	Modèle de correspondance bancaire	56
Figure 12	Les sociétés de services financiers investissent au début de la chaîne de blocs	59
Figure 13	Illustration d'un processus de traçabilité de bout en bout	90
Figure 14	Nombre d'internautes, en millions, 2005-2017	100
Figure 15	Proportion d'internautes (en pourcentage de la population) en 2015	100
Figure 16	Proportion d'internautes (pour 100 habitants)	101
Figure 17	Écart dans l'utilisation d'Internet (pour 100 habitants)	101
Figure 18	Bande passante internationale pour Internet par internaute (en bit/seconde)	102
Figure 19	Prévision de la valeur commerciale des chaînes de blocs	123

Figure A.1	Étapes typiques d'une transaction dans la chaîne de blocs	129
Figure A.2	Composition d'un bloc	132
Figure A.3	Le Tangle	133
Figure A.4	Les « blocs élémentaires » de la chaîne de blocs	133

Tableaux

Tableau 1	Aperçu des principales caractéristiques des différents types de chaînes de blocs	9
Tableau 2	Commission et durée de transaction moyennes, capacité de transaction et efficacité énergétique pour les dix principales cryptomonnaies	106

La chaîne de blocs peut-elle révolutionner le commerce international ?

Le commerce a toujours été façonné par l'innovation technologique. Ces derniers temps, une nouvelle technologie, la chaîne de blocs, a été accueillie par beaucoup comme le prochain grand facteur de changement. La chaîne de blocs peut-elle révolutionner le commerce international ?

Cette publication tente de démythifier le phénomène de la chaîne de blocs en fournissant une explication de base de cette technologie. Elle analyse sa pertinence pour le commerce international en examinant comment elle est actuellement utilisée ou peut être utilisée dans les différents domaines couverts par l'OMC. Ce faisant, elle donne une idée de la mesure dans laquelle cette technologie pourrait affecter le commerce transfrontières des biens et des services et les droits de propriété intellectuelle. Elle examine le potentiel de la chaîne de blocs de réduire les coûts du commerce et d'améliorer la transparence de la chaîne d'approvisionnement, et les possibilités qu'elle offre aux petits producteurs et aux petites entreprises. Enfin, elle passe en revue les divers défis qui doivent être relevés pour que cette technologie puisse être utilisée à grande échelle et ait un impact important sur le commerce international.

