



Conseil économique et social

Distr. générale
17 janvier 2019
Français
Original : anglais

Commission économique pour l'Europe

Comité exécutif

Centre pour la facilitation du commerce et les transactions électroniques

Vingt-cinquième session

Genève, 8 et 9 avril 2019

Point 7 c) de l'ordre du jour provisoire

Recommandations et normes :

Autres produits à noter

Livre blanc : vue d'ensemble des applications pour le commerce de la technologie de la chaîne de blocs

Introduction à l'utilisation de la chaîne de blocs aux fins de la facilitation du commerce

Résumé

La technologie de la chaîne de blocs et la technologie de registre décentralisé de manière générale pourraient sensiblement améliorer la fiabilité des transactions commerciales internationales. Le présent Livre blanc porte sur les principaux aspects de la chaîne de blocs et de son fonctionnement, l'objectif étant de parvenir à une compréhension commune et de jeter les bases de tous les travaux que le Centre des Nations Unies pour la facilitation du commerce et les transactions électroniques (CEFACT-ONU) mènera sur le sujet. Il s'achève par des indications quant à la pertinence, selon le contexte, d'utiliser ou non la chaîne de blocs.

Publié sous la cote ECE/TRADE/C/CEFACT/2019/9, le présent document est soumis par le Bureau du CEFACT-ONU à la vingt-cinquième session de la Plénière pour qu'il en soit pris note.



I. Introduction à l'utilisation de la chaîne de blocs dans le contexte de la facilitation du commerce

A. Introduction

1. Le projet de livre blanc sur la chaîne de blocs du CEFACT-ONU a débouché sur deux Livres blancs consacrés à ce sujet. Le premier, qui traite de l'incidence de cette technologie sur les travaux que le CEFACT-ONU mène dans le domaine des normes techniques, a été publié sous la cote ECE/TRADE/C/CEFACT/2019/8. Le présent document est le deuxième Livre blanc, qui porte sur la manière dont la technologie de la chaîne de blocs pourrait être utilisée pour faciliter le commerce et les processus métier y afférents.

2. Comme expliqué plus loin, l'expression « chaîne de blocs » est utilisée dans l'ensemble du présent document comme synonyme de l'expression « technologie de registre décentralisé ».

3. La technologie de la chaîne de blocs se fonde sur une utilisation innovante de la cryptographie et a suscité beaucoup d'attention en raison de ses caractéristiques, parmi lesquelles figurent :

- La création de fichiers permanents (c'est-à-dire que les fichiers ne peuvent être ni modifiés ni supprimés) ;
- La capacité de déterminer l'heure et l'origine de chaque entrée de la chaîne de blocs ;
- L'accès de tous les participants à l'ensemble des données de la chaîne de blocs ; et
- L'exécution garantie des contrats intelligents (programmes), qui intervient automatiquement dès qu'un ensemble de conditions convenues sont réunies.

4. La chaîne d'approvisionnement internationale se caractérise par des flux de marchandises et de données y relatives. Ces flux et ces données sont liés au mouvement des fonds associés, qui témoignent de la nature transactionnelle des chaînes d'approvisionnement. Généralement, ce mouvement de fonds correspond à des actions précises survenant dans la chaîne d'approvisionnement et s'effectue par voie électronique, de sorte qu'il se prête bien à l'application de la technologie de la chaîne de blocs. Les marchandises vont de l'exportateur à l'importateur en échange de fonds qui vont en sens inverse. Le flux de marchandises et de fonds se fonde sur un flux bidirectionnel de données telles que factures, avis d'expédition, connaissements, certificats d'origine et déclarations d'importation ou d'exportation déposées auprès des organismes de contrôle.

5. Cette description permet de mettre en lumière l'intérêt que présente la technologie de la chaîne de blocs pour le CEFACT-ONU. Depuis les années 1960, le CEFACT-ONU et ses prédécesseurs ont élaboré des recommandations et des normes visant à faciliter le commerce. En outre, depuis l'introduction de la norme EDIFACT¹ dans les années 1980, le CEFACT-ONU a également élaboré et tenu à jour des normes qui visent à faciliter le commerce en améliorant la circulation des données s'y rapportant.

6. Un élément de confiance caractérise chacun des trois flux décrits ci-dessus (flux de biens, de données et de fonds). La confiance – ou l'absence de confiance – a une incidence sur pratiquement toutes les opérations et tous les échanges de données dans le commerce international. Elle concerne notamment :

- L'origine et l'authenticité des biens ;
- La valeur déclarée des biens pour l'assurance, les droits de douane et les paiements ;
- Les promesses de paiement ;

¹ La norme relative à la transmission électronique des données en matière d'administration, de commerce et de transport (EDIFACT) est une norme qui est aujourd'hui largement utilisée dans le transport international, la logistique et d'autres secteurs.

- La protection des biens pendant l'expédition (c'est-à-dire notamment l'intégrité de l'emballage ainsi que l'état du véhicule et du conteneur) ;
- L'intégrité des informations utilisées par les organismes de contrôle aux fins des évaluations des risques qu'ils effectuent en vue des inspections et des autorisations ; et
- Les acteurs du commerce et les prestataires de services qui prennent part à une transaction commerciale.

7. Cet élément de confiance entre les différents agents économiques permet de déterminer les technologies dont on a besoin pour atteindre le niveau de fiabilité souhaité dans les échanges électroniques. Lorsque les partenaires se font confiance, ils peuvent se satisfaire de méthodes d'authentification peu contraignantes. Si tel n'est pas le cas, une procédure d'authentification plus stricte s'impose. La réponse aujourd'hui apportée à cet aspect de confiance(défiance) passe encore largement par des documents papier, des signatures écrites, des primes d'assurance, des fonds entiers et d'autres services fournis par des tiers de confiance.

8. La chaîne de blocs est un type de technologie de registre décentralisé qui fournit des méthodes d'authentification très fiables. Elle pourrait donc permettre de renforcer sensiblement l'élément de confiance mentionné plus haut, et ce souvent plus rapidement que les autres technologies et à moindre coût.

9. Tant la chaîne de blocs que la technologie de registre décentralisé ont le potentiel d'améliorer sensiblement et d'automatiser les processus concernés. Dans la suite du présent document, nous utiliserons uniquement l'expression « chaîne de blocs », étant entendu qu'il s'agit d'une technologie de registre décentralisé.

10. En tant que centre de liaison pour la facilitation du commerce et les normes applicables aux transactions électroniques dans le système des Nations Unies, le CEFACT-ONU doit se poser la question des incidences qu'aura cette nouvelle technologie sur ses deux principaux domaines d'activité. L'incidence de la chaîne de blocs sur les normes du CEFACT-ONU applicables aux transactions électroniques est examinée dans le premier Livre blanc (ECE/TRADE/C/CEFACT/2019/8), tandis que le présent Livre blanc porte sur l'incidence de la chaîne de blocs sur la facilitation du commerce. De nombreux secteurs commerciaux ont été étudiés, dans la mesure où ceux-ci ont élaboré leurs propres mécanismes de confiance. En effet, le degré de confiance requis varie d'un secteur à l'autre et au fil du temps. On ne peut donc pas examiner l'utilisation de la chaîne de blocs dans tous les types de commerce comme si les besoins et les défis étaient toujours les mêmes. Une liste des secteurs examinés est présentée ci-après, et les résultats des études menées sont décrits dans le document « Blockchain in Trade Facilitation: Sectoral Challenges and Examples » (ECE/TRADE/C/CEFACT/2019/INF.3). Ce document s'articule autour des secteurs horizontaux et verticaux suivants :

- Secteurs horizontaux :
 - La sécurité de la chaîne de blocs et les aspects juridiques et réglementaires ; et
 - La chaîne de blocs à l'appui des objectifs de développement durable des Nations Unies.
- Secteurs verticaux :
 - Les chaînes d'approvisionnement, la traçabilité et la chaîne de blocs ;
 - Les transports maritimes et la chaîne de blocs ;
 - Les transports non maritimes et la chaîne de blocs ;
 - Le commerce agricole et la chaîne de blocs ;
 - Les services financiers et la chaîne de blocs ;
 - Les services publics et la chaîne de blocs ;
 - Le tourisme et la chaîne de blocs ;
 - La musique et les arts et la chaîne de blocs ; et

- Les services de santé et la chaîne de blocs.

11. En outre, le modèle figurant en annexe a permis de recueillir des informations sur les cas d'utilisation et l'application effective de la chaîne de blocs.

B. Prochaines étapes

12. L'équipe de projet du CEFACT-ONU chargée du Livre blanc sur la chaîne de blocs s'est physiquement réunie en octobre 2018 dans le cadre du Forum de Hangzhou (Chine). Lors de cette réunion, les membres de l'équipe se sont accordés à dire que l'un des effets les plus positifs du projet a été la possibilité pour ceux qui utilisent la technologie de la chaîne de blocs ou envisagent de le faire d'avoir des discussions concrètes sur les possibilités d'application, les options de substitution, les problèmes pouvant se poser et les solutions éventuelles. Il existe de nombreux forums et conférences consacrés à la technologie de la chaîne de blocs, mais ceux-ci sont principalement axés sur les questions relatives à la cryptomonnaie ou à l'investissement, n'offrent guère la possibilité de dialoguer (c'est-à-dire qu'ils servent principalement à faire circuler des informations) et sont dominés par les discours de ceux qui cherchent à vendre et à promouvoir des solutions s'appuyant sur la chaîne de blocs.

13. Sur cette base, l'équipe de projet a proposé d'organiser un forum pour discuter de l'utilisation de la chaîne de blocs dans la chaîne d'approvisionnement internationale et de son extension à d'autres technologies de pointe telles que l'Internet des objets et l'intelligence artificielle. Ce forum pourrait éclairer les cadres supérieurs chargés de prendre des décisions concernant les applications de la chaîne d'approvisionnement internationale, en particulier au niveau des gouvernements. Il pourrait également aider le CEFACT-ONU à recenser les domaines dans lesquels ses travaux pourraient faciliter l'utilisation de ces technologies de pointe à l'appui de la facilitation du commerce.

14. L'équipe de projet a appuyé une proposition tendant à créer un groupe consultatif sur le recours aux technologies de pointe dans la chaîne d'approvisionnement internationale² qui appuierait la mise en œuvre du programme de travail du CEFACT-ONU dans les domaines d'activités liés à l'utilisation des technologies numériques aux fins de l'échange d'informations commerciales. Ce groupe consultatif aurait pour mission principale de mettre en lumière les nouvelles questions stratégiques et les meilleures pratiques internationales dans ce domaine à l'intention des hauts fonctionnaires et des hauts responsables du secteur privé. L'une de ses premières tâches consisterait à examiner les questions soulevées dans les analyses sectorielles et les études de cas exposées dans le présent Livre blanc. Sur la base de ce travail, le groupe consultatif formulerait des recommandations concernant les travaux futurs ainsi que des lignes directrices et des documents d'information à soumettre au CEFACT-ONU pour examen et adoption éventuelle.

II. Qu'est-ce que la chaîne de blocs et quels en sont les différents types ?

A. Histoire et contexte

15. Bien que certains des principes de la technologie de la chaîne de blocs aient déjà été décrits dans des documents antérieurs sur la cryptographie, le fondement de cette technologie telle qu'elle est utilisée aujourd'hui a été présenté pour la première fois en octobre 2008 dans un Livre blanc envoyé à une liste de diffusion consacrée à la cryptographie. Le document, intitulé « Bitcoin: A Peer-to-Peer Electronic Cash System », avait été publié par un auteur, ou un groupe d'auteurs, sous le pseudonyme « Satoshi Nakamoto ». Il est intéressant de noter que dans le document original, ce n'était pas

² Voir proposition intitulée « Mandat et cahier des charges du groupe consultatif sur les technologies de pointe » ECE/TRADE/C/CEFACT/2019/22.

l'expression « chaîne de blocs » qui était utilisée, mais plutôt des expressions telles que « blocs enchaînés ». La première utilisation de l'expression « chaîne de blocs » est apparue sur la même liste de diffusion lors de discussions ultérieures liées au document original de Nakamoto.

16. Le 9 janvier 2009, Satoshi Nakamoto a publié, sur le site du logiciel libre SourceForge, la version 0.1 du logiciel Bitcoin, premier instrument dans lequel étaient mis en œuvre les principes décrits dans le document d'octobre 2008.

17. Satoshi Nakamoto a continué de collaborer avec d'autres développeurs sur le logiciel Bitcoin jusqu'à la mi-2010. À cette époque, il a confié le contrôle du référentiel du code source et de la clef d'alerte à Gavin Andresen et transféré plusieurs noms de domaines connexes à d'autres membres éminents de la communauté Bitcoin, avant de quitter le projet. L'identité de Satoshi Nakamoto a nourri les spéculations jusqu'à ce jour mais, en dépit du travail d'enquête fait à ce sujet, on ignore toujours qui se cache derrière cette identité.

18. Un autre important jalon dans le développement de la technologie de la chaîne de blocs a été la mise au point de chaînes de blocs capables d'exécuter de petits programmes informatiques appelés contrats intelligents qui exploitent un langage de programmation complet (appelé langage de programmation « Turing-complet »).

19. Les contrats intelligents ont permis à la chaîne de blocs d'exécuter un ensemble varié de fonctions impliquant un transfert d'informations ou de valeur, tout en laissant des traces transparentes et fiables permettant d'en suivre le parcours. De plus amples informations sur les contrats intelligents sont données plus loin dans le présent document.

20. Ethereum a été le premier concept basé sur la chaîne de blocs à utiliser les contrats intelligents. Son créateur, Vitalik Buterin, a décrit pour la première fois dans un Livre blanc paru fin 2013 l'utilisation de contrats intelligents dans une chaîne de blocs. N'ayant pas recueilli l'adhésion de la communauté Bitcoin, il a développé sa propre plateforme appelée Ethereum. Celle-ci, lancée le 30 juillet 2015, est aujourd'hui la chaîne de blocs qui compte le plus grand nombre de transactions. Elle figure dans le trio de tête en termes de capitalisation boursière³.

B. Les modalités de fonctionnement de la chaîne de blocs

21. Au cœur d'une chaîne de blocs, on trouve un protocole cryptographique qui permet à des parties distinctes de renforcer la fiabilité d'une transaction, car les entrées de la base de données sont difficilement piratables (c'est-à-dire qu'une fois les données consignées, il est pratiquement impossible de les modifier). Cette « immuabilité » s'explique par une combinaison de facteurs, parmi lesquels figurent les méthodes cryptographiques utilisées dans la chaîne de blocs, son mécanisme de consensus et de validation ainsi que sa nature décentralisée. En raison de cette immuabilité, les systèmes fondés sur la chaîne de blocs peuvent servir d'arbitres indépendants dans des processus qui pourraient autrement exposer les participants au risque de non-respect par une partie de ses obligations contractuelles (risque de contrepartie) et dans lesquels les tiers garants hésitent à intervenir et à assumer une partie du risque.

22. L'objectif du présent document n'est pas de proposer un examen approfondi de la technologie de la chaîne de blocs : les lecteurs pourront consulter les nombreuses ressources Web pour ce faire. Il s'agit plutôt de présenter les concepts fondamentaux dont on a besoin pour comprendre de quelle manière la chaîne de blocs pourrait être appliquée aux chaînes d'approvisionnement internationales.

23. Avant toute chose, il convient de proposer quelques définitions :

a) Bloc : Données qui sont ajoutées au registre après validation. Une fois un bloc incorporé à la chaîne, il ne peut être ni modifié ni supprimé sans que tous les blocs suivants soient remplacés ;

³ D'après <https://bitinfocharts.com/> (décembre 2018).

b) Consensus : Caractéristique importante des systèmes fondés sur la chaîne de blocs qui permet aux utilisateurs de savoir que des transactions ont été exécutées et d'évaluer la fiabilité des informations relatives à ces transactions ou inhérentes à celles-ci (par exemple, la date et l'heure de l'exécution et le contenu de la transaction). Dans le cas des chaînes de blocs publiques, l'arbitre qui permet de parvenir à un consensus est le réseau de tous les nœuds qui choisissent de participer. Dans le cas des chaînes de blocs privées, l'arbitre est le consortium de l'ensemble des nœuds habilités à former un consensus. De plus amples informations sur les différentes manières dont le consensus peut être atteint sont données plus loin dans le document ;

c) Monnaie fiduciaire : devises émises par une banque centrale comme le dollar, l'euro, le yen, etc. ;

d) Hash : résultat des opérations mathématiques effectuées sur la représentation numérique des données (toutes les données d'un ordinateur sont des chiffres qui sont décodés afin de créer les mots et les images que l'on voit à l'écran). De taille fixe, ce résultat constitue l'empreinte cryptographique unique des données sous-jacentes. Le hachage est une fonction unidirectionnelle, ce qui veut dire qu'il est facile de remonter au hash à partir des données. Pour ce faire, on effectue des opérations mathématiques prédéfinies sur les données qui sont censées être à l'origine du hash : si le résultat est le même, les données sont identiques. Il s'agit là d'une caractéristique clef, car elle permet aux utilisateurs de confirmer rapidement qu'aucun changement d'aucune sorte n'a été apporté. Par exemple, même un espace supplémentaire ou une ligne vide dans un texte modifierait son hash. Dans le même temps – et c'est ce qui fait que le hachage est une fonction unidirectionnelle –, il est pratiquement impossible de recréer les données d'origine à partir du seul hash (c'est-à-dire de procéder à une ingénierie inverse) ;

e) Nœud : système qui héberge une copie complète du registre de la chaîne de blocs. Dans certaines chaînes de blocs telles que Bitcoin et Ethereum, tous les nœuds participent au processus de consensus, tandis que dans d'autres, seuls le font des nœuds sélectionnés ;

f) Transaction dont le résultat est inscrit sur la chaîne de blocs (on-chain transaction) : procédure automatisée qui crée ou met à jour le statut d'un actif de la chaîne de blocs dans la base de données en ajoutant de nouvelles données au registre. L'échange d'actifs numériques ou l'exécution d'un processus métier automatisé en sont des exemples.

g) Validation : travail effectué par les nœuds, chacun de leur côté, qui permet de vérifier toutes les transactions à l'aide d'un algorithme de consensus. Différents réseaux peuvent utiliser différents algorithmes de consensus. Lorsque la validation mutuelle aboutit à un consensus, les nœuds inscrivent (enregistrent) les transactions vérifiées sur leur chaîne de blocs en tant que nouveau bloc.

1. La chaîne de blocs est une technologie de registre décentralisé

24. Les registres sont des listes d'écritures où les transactions sont enregistrées une seule fois et ne peuvent pas être mises à jour par la suite. Cela signifie que toute modification doit être enregistrée en tant que nouvelle transaction (comme pour les écritures comptables). Les registres numériques peuvent être stockés sous la forme d'une base de données, également appelée journal de données. Chaque écriture peut être lue plusieurs fois mais ne peut être écrite qu'une seule fois. Le terme « registre » est tiré de la comptabilité où les écritures, une fois inscrites dans un registre (grand livre comptable), ne peuvent plus être modifiées. Une base de données en chaîne de blocs est un registre parce qu'elle utilise des hashes pour garantir qu'aucune des données qu'elle contient n'a jamais été modifiée.

25. Une base de données en chaîne de blocs est décrite comme étant décentralisée, car plusieurs copies des données sont conservées sur plusieurs nœuds à la fois. Les multiples copies sont mises à jour avec l'introduction de nouveaux blocs de données d'une manière coordonnée, permettant d'assurer le maintien de leur cohérence grâce à un algorithme de consensus dont il existe différents types.

26. En résumé, le contenu et la séquence des blocs de données dans une chaîne de blocs sont déterminés par un consensus entre les nœuds participants, et chaque bloc contient une

empreinte digitale (hash) qui peut être utilisée pour vérifier de manière récursive le contenu de tous les blocs précédents.

2. Les transactions sont consignées sur la chaîne de blocs

27. Chaque bloc de données consigné sur un registre de la chaîne de blocs contient au moins une transaction, bien que la plupart des blocs en contiennent plusieurs. Par exemple, une transaction simple consiste à débiter une pièce du compte A pour la créditer sur le compte B, bien que de nombreux autres types de transactions soient possibles. Certaines chaînes de blocs contiennent un sous-ensemble limité de transactions (opérations ou algorithmes), comme cette simple opération comptable en partie double. D'autres contiennent un ensemble beaucoup plus large de transactions couvrant tout algorithme calculable (c'est-à-dire un langage de programmation informatique complet de Turing⁴). Ces types de transactions portent différents noms : contrats intelligents, chaînes de code, familles de transactions ou autres termes équivalents. En résumé, toutes les chaînes de blocs se prêtent à une variété d'opérations de données, mais les chaînes de blocs ne s'accroissent pas toutes des langages de transaction complets de Turing.

3. Ces transactions sont consignées dans un bloc crypté

28. Les chaînes de blocs s'appuient sur deux types de technologie cryptographique : la fonction de hachage et la cryptographie à clef publique ou privée. La fonction de hachage est utilisée pour construire la preuve fondamentale qui relie chaque bloc au reste de la chaîne qui le précède. Dans un contexte différent, les hashes peuvent aussi être utilisés pour fournir une preuve de validité des données référencées par les blocs. Ils sont également utilisés dans les algorithmes de preuve de travail, où un hash commençant par un certain nombre de zéros sert de « problème difficile » que les nœuds doivent résoudre pour obtenir un consensus.

29. La cryptographie à clef publique ou privée est utilisée pour identifier les parties à une transaction et contrôler l'accès aux données. On peut faire l'analogie avec le courrier électronique, où la clef publique est l'adresse électronique que les autres peuvent utiliser pour envoyer des messages, et la clef privée le mot de passe qui donne accès au matériel privé, c'est-à-dire le message. Sur une chaîne de blocs, une clef publique peut ainsi être utilisée, par exemple, pour exécuter une transaction qui correspond à l'envoi d'un document ou d'un paiement à une partie, étant entendu que seule la partie ayant la clef privée peut accéder à ce document ou ce paiement après l'envoi.

4. Des nœuds indépendants doivent vérifier le bloc crypté

30. Les systèmes fondés sur la chaîne de blocs utilisent différents algorithmes de consensus. Bitcoin, qui est une chaîne de blocs publique, utilise par exemple des algorithmes de preuve de travail qui permettent aux mineurs de recevoir des frais de transaction en échange des calculs coûteux réalisés, et ces frais permettent également de mettre des pièces en circulation. Les registres accessibles sur autorisation utilisent un consortium de nœuds – qui jouissent d'une confiance collective mais pas nécessairement d'une confiance individuelle – pour s'entendre sur le résultat d'un processus de consensus, ce qui est généralement moins coûteux et plus rapide que la preuve de travail de Bitcoin. Tous les processus de consensus nécessitent un mécanisme permettant de résoudre les conflits ou de lever les incertitudes quant au prochain bloc qui devrait être ajouté à la chaîne. La plupart de ces mécanismes sont fondés sur l'utilisation du bloc, qui doit être approuvé par plus de 50 % des nœuds. De plus amples informations sur les chaînes de blocs publiques et accessibles sur autorisation sont données plus loin.

31. La nature du mécanisme de consensus détermine certaines caractéristiques clefs d'un système fondé sur la chaîne de blocs. Par exemple, le minage de blocs a délibérément

⁴ Un langage de programmation complet de Turing peut résoudre n'importe quel problème mathématique par le calcul (si l'on sait comment le programmer). D'une manière générale, cela signifie qu'il doit être capable d'exécuter une répétition conditionnelle ou un saut conditionnel (*while*, *for*, *if* et *goto*) ainsi que de lire et d'écrire dans un mécanisme de stockage (variables).

été rendu coûteux. Cela permet de protéger la chaîne de blocs, car le coût qu'entraîne le contrôle de plus de 50 % des nœuds, soit le nombre nécessaire pour valider un bloc et donc manipuler toute la chaîne, est prohibitif. Pour compenser ce coût, les mineurs sont récompensés à la fois par un montant de bitcoins pour chaque bloc créé et par les frais de chaque transaction confirmée par leurs soins dans la chaîne de blocs⁵. La taille de chaque bloc est limitée, et les coûts de transaction sont déterminés par le marché, de sorte que plus le nombre de transactions demandées est élevé, plus le prix de chacune d'entre elles augmente. Un tel modèle est nécessaire pour le fonctionnement économique du Bitcoin, qui cherche à parvenir à un consensus honnête sur un marché non réglementé d'opérateurs potentiellement anonymes et économiquement rationnels (c'est-à-dire des opérateurs qui, étant anonymes et n'encourant aucun frais ce faisant pourraient voler des actifs). Qui plus est, si un nœud (ou un mineur) n'accepte pas le bloc validé par plus de 50 % des autres nœuds, il est de fait exclu de la chaîne de blocs, perdant ainsi la possibilité de gagner de futurs bitcoins et d'engranger des frais de transaction. Par conséquent, la bande passante du Bitcoin est extrêmement faible en raison du coût de création des blocs, les transactions prenant en moyenne dix minutes à être validées. En outre, du fait du très grand nombre de nœuds et d'utilisateurs, qui génèrent d'importantes quantités de données, ainsi que de la taille limitée des blocs, il serait très coûteux et peu rentable de stocker des données sur la chaîne de blocs Bitcoin.

32. Étant donné que les informations sont copiées sur tous les nœuds d'une chaîne de blocs, il est généralement peu rentable de stocker des quantités importantes de données sur les chaînes de blocs. Des milliards de dollars des États-Unis de transactions en bitcoins et d'autres transactions de grande valeur s'effectuent encore sur Bitcoin, mais en raison de ses capacités limitées en termes de vitesse et de volume, la plateforme ne se prête pas à de nombreuses applications d'entreprise et à l'exécution directe de transactions de petits montants.

33. Pour les registres accessibles sur autorisation, l'équilibre entre la largeur de bande, la capacité et la fiabilité est différent. Dans ces registres qui permettent davantage de contrôler qui participe, par exemple, d'autres mécanismes de consensus peuvent être utilisés, même si certains d'entre eux sont un peu moins solides que la preuve de travail utilisée par Bitcoin. C'est ainsi qu'il existe des mécanismes de consensus fondés sur le montant qu'un nœud a investi dans un réseau (ce que l'on appelle la preuve de participation) ou des mécanismes dans lesquels le consensus d'un sous-ensemble de nœuds est validé par un groupe plus large.

34. En outre, les fondations, les universités et les entreprises font un gros travail de recherche pour trouver et mettre à l'essai d'autres mécanismes de consensus. Certains de ces autres mécanismes devraient permettre de traiter des centaines, voire des milliers de transactions par seconde, contrairement à Bitcoin qui crée un nouveau bloc par intervalles de dix minutes. Des recherches sont également menées sur la maintenance des bases de données à l'échelle du pétaoctet (c'est-à-dire des bases de données vraiment gigantesques) et sur l'accès aux données dans de telles bases.

5. Le bloc est inscrit dans le registre après vérification

35. Lorsqu'un consensus est atteint, ce qui signifie que l'on s'accorde sur le fait que le bloc contient des données légitimes et que c'est celui-ci qui sera le prochain à être agrégé, chaque nœud ajoute le nouveau bloc à sa copie locale du registre. Ainsi, tous les nœuds conservent une copie identique du registre chaque fois qu'un nouveau bloc est créé. La preuve en est que chaque bloc inscrit au registre contient le hash du bloc qui le précède.

6. Le nouveau bloc est lié aux blocs précédents, ce qui crée une immuabilité

36. Rappelons que le hachage est une fonction unidirectionnelle qui permet de créer une empreinte digitale unique des données sélectionnées. Cette fonction produit une empreinte

⁵ Le Bitcoin est conçu de manière que, avec le temps, les récompenses associées au minage soient réduites, l'objectif final étant que les mineurs soient récompensés uniquement par des frais de transaction.

de taille fixe quelle que soit la quantité de données hachées. Par conséquent, il n'y a aucun moyen de savoir, en regardant le hash, si les données étaient un seul petit document ou une base de données contenant plusieurs milliards d'entrées.

37. Chaque bloc d'une chaîne contient les données relatives à une transaction ainsi que le hash du bloc précédent, qui fait toujours la même taille quelle que soit la quantité de données qu'il représente. Étant donné qu'il y a consensus sur le fait que ce nouveau bloc fait partie de la chaîne, il est possible de vérifier le bloc précédent à partir de son hash, puis le bloc qui le précède à partir de ce bloc, et ainsi de suite jusqu'au premier bloc de la chaîne, appelé « bloc de genèse ». On dit du hash du bloc précédent qu'il est ancré dans le bloc suivant.

38. Le fait d'altérer le contenu d'un bloc de la chaîne aura pour effet de modifier le hash de ce bloc, ce qui modifiera le hash du bloc suivant, et ainsi de suite pour chaque bloc suivant de la chaîne. Si cela devait se produire, n'importe quel nœud détecterait facilement la manipulation, et les algorithmes de consensus empêcheraient la création de nouveaux blocs dans la chaîne parce que les hashes ne correspondraient pas.

39. Cette caractéristique est à l'origine du mot « chaîne » dans l'expression « chaîne de blocs », car chaque bloc est ancré au bloc précédent et prouve l'existence de toutes les données référencées en remontant jusqu'au premier « bloc » de données dans la « chaîne ».

C. Types de chaînes de blocs

1. Registres publics

40. Les registres publics peuvent être lus par tout un chacun. Ils sont également accessibles sans autorisation, car tout le monde peut participer aux mécanismes de consensus et utiliser ces mécanismes sans avoir besoin d'une autorisation pour ce faire et sans qu'il soit nécessaire de faire appel à un organisme de réglementation pour faire respecter les règles. Bitcoin, Ether et toute une série d'autres cryptomonnaies dont les capitalisations boursières avoisinent les 59 milliards de dollars⁶ fonctionnent de cette façon : elles autorisent l'ensemble des transactions logiquement valides qui sont conclues entre les membres du réseau, y compris les membres anonymes et ceux qui se présentent sous un pseudonyme.

41. L'une des craintes apparues au sujet de la technologie de la chaîne de blocs est la suivante : si un acteur malveillant réussissait à prendre le contrôle de la majorité des nœuds, il pourrait ensuite décider de créer un consensus contraire aux intérêts des autres parties prenantes. Dans le jargon des spécialistes de la cryptographie, cette menace est appelée « attaque Sybil ». Une attaque Sybil réussie contre une cryptomonnaie fondée sur une chaîne de blocs publique pourrait entraîner une redistribution des actifs ou une double dépense, avec les conséquences catastrophiques que l'on imagine. Les registres des chaînes de blocs publiques sont conçus pour fonctionner selon des règles qui n'exigent pas l'intervention de mécanismes de gouvernance ou de réglementation pour prévenir les transactions malveillantes, parce que ces mécanismes pourraient eux-mêmes être manipulés à des fins malveillantes (si un mécanisme de gouvernance était piraté par une tierce partie ou utilisé de façon abusive par un organisme de réglementation de confiance par exemple). Les chaînes de blocs publiques supposent une confiance absolue en leurs algorithmes et sont conçues pour éviter d'avoir à s'en remettre à des contreparties. C'est la raison pour laquelle on dit parfois que les chaînes de blocs publiques ne requièrent pas de tiers de confiance.

42. D'habitude, les registres publics font l'impasse sur d'autres aspects de la performance afin d'être en mesure de mieux résister aux attaques Sybil. Ils reposent en outre sur leur propre transparence et sur celle des logiciels open-source concernés.

⁶ <https://bitinfocharts.com/>, consulté le 8 décembre 2018 à 14 heures.

2. Registres privés ou accessibles sur autorisation

43. À l'instar des bases de données conventionnelles, le contenu du registre d'une chaîne de blocs peut être un secret gardé qui n'est accessible qu'à certains utilisateurs choisis et à des opérateurs de nœuds au moyen d'un mécanisme de contrôle d'accès selon le rôle. De même, une chaîne de blocs privée peut être configurée pour que chacun puisse lire les données, la possibilité d'en créer de nouvelles étant toutefois réservée à certains nœuds seulement. Ceci vaudrait également pour une base de données publique utilisant des contrats intelligents, les autorités responsables devant cependant savoir qu'elles s'exposent à de plus grands risques pour la sécurité, puisque n'importe qui pourrait voir (et essayer de pirater) les contrats intelligents en question. Une telle base de données pourrait convenir pour stocker des documents officiels tels que des titres fonciers, des licences et des certificats par exemple. À la différence d'une base de données traditionnelle, une chaîne de blocs privée est immuable (c'est-à-dire qu'elle ne peut pas être mise à jour), et les transactions sont vérifiées au moyen d'un mécanisme de consensus établi par les opérateurs du réseau.

44. La technologie du registre privé est généralement utilisée pour les besoins des entreprises souhaitant opérer des transactions immuables qui peuvent être vérifiées par une communauté fermée de nœuds. Ces nœuds peuvent être sans lien avec les parties aux transactions effectuées sur la chaîne de blocs et peuvent faire l'objet d'une surveillance ou d'une gouvernance qui n'est pas possible – ou jugée non souhaitable – dans une chaîne de blocs publique accessible sans autorisation.

45. Les registres accessibles uniquement sur autorisation ne s'appuient pas sur le même modèle de menace que les registres publics. Les opérateurs des nœuds formant les registres accessibles sur autorisation ne sont pas anonymes : ils sont soumis à une sorte de contrôle de gouvernance et jouissent de la confiance collective des utilisateurs. Le comportement malveillant d'un nœud ou d'un participant pourrait conduire à l'éviction du fautif et au blocage de ses transactions. Les utilisateurs d'un registre accessible sur autorisation comptent sur les opérateurs pour intervenir en cas de comportement malveillant et escomptent que ceux-ci ne se laisseront pas aller eux-mêmes à des comportements malveillants.

46. En ce qui concerne les registres accessibles sur autorisation, le niveau de sécurité (et donc la confiance que les utilisateurs peuvent avoir dans l'immutabilité des données) varie selon les règles établies pour ce type de registre, notamment son mécanisme de consensus. Les registres accessibles sur autorisation peuvent aussi créer un sentiment erroné de sécurité, dans la mesure où seuls les participants de confiance sont autorisés à assurer la maintenance des nœuds et à participer aux vérifications nécessaires. Toutefois, même les participants de confiance peuvent en être indignes dès lors qu'ils ont été piratés. En effet, les registres accessibles sur autorisation qui présentent un point de défaillance isolé sont également vulnérables s'il arrive quoi que ce soit à ce point isolé, et des conséquences fâcheuses pour les participants peuvent découler de contrats intelligents n'ayant pas subi d'épreuves suffisantes de mise à l'essai – même s'il n'y avait pas volonté de nuire à l'origine –, en particulier si le réseau de la chaîne de blocs ne dispose pas de mécanismes de contrôle adéquats.

3. Systèmes « inter-registres » : exécution d'opérations d'une chaîne de blocs à l'autre

47. Il existe aujourd'hui de nombreuses chaînes de blocs différentes et, à l'avenir, il y en aura encore plus. Déjà maintenant, une transaction de la chaîne d'approvisionnement, du début à la fin, peut nécessiter l'écriture ou la lecture de données provenant de plusieurs chaînes de blocs. Par exemple, l'exportateur peut avoir besoin d'utiliser une chaîne de blocs du secteur bancaire et une autre pour chaque mode de transport, tandis que l'importateur aura recours à une chaîne de blocs à des fins de traçabilité et les organismes réglementaires à une ou plusieurs autres chaînes de blocs. En outre, il est facile de prévoir un besoin croissant d'échange d'informations et d'exécution de transactions d'une chaîne de blocs à une autre (systèmes inter-registres).

48. La chaîne de blocs offre la possibilité de référencer des données externes telles que des données d'autres chaînes de blocs et des données ne provenant pas de systèmes faisant appel à la chaîne de blocs. Deux grandes catégories de liens vers des données externes

peuvent être concernées dans une chaîne de blocs : les données liées et les transactions entre différentes chaînes de blocs.

49. Les données liées reposent sur l'utilisation de hashes et aussi parfois d'identifiants numériques et de la cryptographie à clef publique. Ce mécanisme fonctionne tant que les règles sont appliquées de manière cohérente dans l'ensemble de la chaîne de blocs et dans le(s) système(s) sur lequel (lesquels) les données liées sont stockées. Cela signifie que plus l'utilisation de la cryptographie à clef publique deviendra la norme, plus il sera facile et moins il sera coûteux de lier les données. Il en va de même pour la sémantique des données. L'utilisation d'une sémantique commune (c'est-à-dire la définition des données) simplifie considérablement l'interprétation des données provenant de différentes sources, et la librairie des composants communs du CEFACT-ONU est une bibliothèque très complète de données relatives au commerce qui peut être utilisée dans ce contexte.

50. Les liens dans une chaîne de blocs qui pointent vers des données externes (également appelées ancres) peuvent également contenir des informations telles que des hashes qui doivent être utilisées pour prouver que les données référencées existent ou qu'elles demeurent inchangées. Cela diffère d'un hyperlien ou d'un localisateur de ressources uniformes (URL) sur Internet, où l'information disponible à une adresse peut changer selon le moment où on la consulte. Par exemple, si l'on clique sur le lien du site Web d'un journal télévisé, qui change régulièrement à mesure qu'il est mis à jour, ce qui y est affiché change d'un jour à l'autre. Avec l'ancrage des données dans la chaîne de blocs, les informations contenues dans la chaîne de blocs sont la garantie (preuve d'existence) du fait que les données vers lesquelles on pointe n'ont pas été modifiées.

51. En plus de lier les données entre deux chaînes de blocs et de pointer vers des données qui peuvent être utilisées par un contrat intelligent (par exemple un certificat d'essai) dans une base de données plus normalisée, les données liées peuvent également être utilisées pour intégrer des mégadonnées hors chaîne dans l'espace restreint d'une chaîne de blocs. Des données supplémentaires peuvent être stockées soit dans des systèmes de données décentralisés qui sont publics ou ouverts tels que le système de fichier interplanétaire (IPFS) – mémoire ouverte et adressable par contenu qui utilise des protocoles Internet standard –, soit dans des bases de données privées qui sont accessibles seulement à certains utilisateurs autorisés du registre. Grâce aux liens hors chaîne ou aux liens entre plusieurs chaînes, les opérateurs du réseau peuvent savoir que certaines données existent, mais leur accès à ces données est limité par des contrôles supplémentaires. Ce système peut être très intéressant du point de vue de la protection de la vie privée, car il est possible d'accéder aux données pour vérifier, par exemple, si une personne a plus de 21 ans sans que son âge exact soit fourni, ou pour vérifier si elle vit à Londres sans que son adresse soit fournie.

52. Ces sources de données externes sont parfois appelées oracles et sont décrites plus en détail ci-dessous.

53. Les transactions inter-registres (qui couvrent plusieurs chaînes de blocs) utilisent des liens entre chaînes de blocs et des contrats intelligents (voir description ci-dessous) sur les deux chaînes de blocs qui interagissent de manière coordonnée. Il s'agit d'un domaine nouveau, mais il existe des mécanismes qui sont déjà utilisés. Ces mécanismes, comme par exemple Ripple Interledger et Lightning Network, sont principalement axés sur l'échange de valeur (c'est-à-dire d'actifs numériques) entre les registres.

D. Les contrats intelligents, les oracles et l'application de la chaîne de blocs à l'Internet des objets

1. Les contrats intelligents

54. Les contrats intelligents sont des programmes informatiques à exécution automatique qui codent la logique métier. Ils s'auto-exécutent lorsque des conditions prédéfinies sont remplies. En d'autres termes, ce n'est pas un être humain qui lance leur exécution, ou du moins pas directement. Il peut s'agir d'une action simple telle que le transfert d'un certain montant d'actifs d'un compte X à un compte Y. Les contrats

intelligents fonctionnent sur le modèle conditionnel IFTTT (de l'anglais *If-This-This-Then-That*), selon lequel une instruction est automatiquement exécutée lorsque certaines conditions sont remplies. Il peut s'agir d'un laps de temps défini, d'une valeur donnée (par exemple le prix de certains actifs tels qu'un titre) ou d'un événement particulier, comme la livraison de marchandises à un client qui les a commandées.

55. Les contrats intelligents offrent plusieurs avantages :

- Ils renforcent la sécurité et améliorent la prévisibilité, car ils se passent de l'élément humain et préviennent les violations de contrat, intentionnelles ou non, qui pourraient être causées par une intervention humaine ;
- Ils améliorent la transparence, car le code d'un contrat intelligent peut être public et visible, et n'importe qui peut l'examiner et prédire la manière dont les transactions seront effectuées dans le cadre d'un contrat donné ; et
- Le langage de programmation est simplifié pour les systèmes qui ont besoin d'accepter et d'apparier des données provenant d'une grande variété de parties, dont plusieurs peuvent être inconnues, et d'exécuter une action à partir de ces données.

56. Dans le langage courant, on pourrait décrire les caractéristiques des contrats intelligents comme suit :

- **Condition préalable** : je dépose une certaine quantité de cryptomonnaie et l'autre partie dépose une certaine quantité de monnaie fiduciaire ;
- **Condition** : les montants doivent être égaux selon les taux de change du moment ;
- **Action** : les devises sont alors échangées entre les comptes des parties concernées.

57. Une autre illustration possible est celle de la location d'une voiture. Si l'agence de location exige le versement d'un acompte sur une chaîne de blocs, le montant ne sera versé à l'agence qu'une fois que le loueur aura confirmé qu'il a reçu les clés du véhicule. De cette manière, les contrats intelligents peuvent prévenir les perceptions indues d'acomptes et créer un élément d'assurance supplémentaire.

58. Étant donné que les contrats intelligents portent en fait sur de petits programmes, ils peuvent être développés et personnalisés au gré de situations diverses, ce qui en fait des outils potentiellement puissants pour les entreprises.

2. Les oracles

59. La fonction première des oracles est de fournir des données sécurisées et fiables à un contrat intelligent dans une chaîne de blocs. Les contrats intelligents examinent ensuite ces données pour voir si elles remplissent les conditions définies dans leur code et, si tel est le cas, le contrat s'auto-exécute.

60. Les mots d'ordre sont ici la sécurité et la fiabilité des données. Les chaînes de blocs ne peuvent pas, et ne devraient pas, stocker de grandes quantités de données, de sorte que les informations doivent être soumises à la chaîne de blocs via un oracle. De ce fait, l'oracle (tout comme les interfaces utilisateur) représente un point faible dans la sécurité et l'intégrité d'une chaîne de blocs. Comme il est coutume de le dire, « à données douteuses, résultats douteux », et dans le cas des chaînes de blocs, on pourrait dire « à données faussées, résultats définitivement faussés ». Par conséquent, il est très important, dans les applications fondées sur la chaîne de blocs, de bien concevoir le processus d'obtention des données utilisées par les oracles ainsi que l'interface entre l'oracle et la chaîne de blocs afin de garantir la qualité et l'intégrité des données et des processus associés.

3. L'Internet des objets et la chaîne de blocs

61. L'Internet des objets fait référence aux capteurs et aux petits dispositifs informatiques ou puces intégrés dans des objets physiques qui communiquent par Internet. Ceux-ci peuvent communiquer entre eux ou avec des ordinateurs et des systèmes informatiques de plus grande taille, ou même avec des humains, à l'instar des systèmes de sécurité modernes qui, s'ils détectent un mouvement dans la maison, en avertissent le propriétaire et le connectent à la caméra vidéo du salon.

62. Les dispositifs reliés à l'Internet des objets peuvent recueillir une grande variété de données. Parmi les exemples d'informations relatives au commerce et au transport communiquées par de tels dispositifs, on peut citer la localisation et le suivi des déplacements des camions ou des conteneurs grâce aux coordonnées GPS, l'ouverture et la fermeture des portes des conteneurs, le contrôle de la température des conteneurs, la détection des chocs extérieurs pouvant endommager les conteneurs, les palettes ou les produits ainsi que, pour les articles très coûteux comme certains produits pharmaceutiques ou produits de luxe, le suivi ou l'identification des colis ou produits individuels.

63. Les dispositifs reliés à l'Internet des objets peuvent être un bon moyen de recueillir des données analysées par d'autres systèmes qui fournissent ensuite les résultats des analyses à une chaîne de blocs (c'est-à-dire des systèmes qui font office d'oracles pour une chaîne de blocs), à moins qu'ils ne soient eux-mêmes des oracles en fournissant directement des données à une chaîne de blocs. Néanmoins, on a tendance à ne pas utiliser les dispositifs reliés à l'Internet des objets directement comme des oracles parce qu'il peut y avoir des problèmes de sécurité et que les systèmes connectés à des dizaines de milliers d'appareils reliés à l'Internet des objets peuvent être saturés par de trop grands volumes de données. En outre, la constante écriture de données dans une chaîne de blocs peut s'avérer coûteuse dans des réseaux où chaque nouvelle écriture implique le paiement d'un petit montant. Par conséquent, les données des dispositifs reliés à l'Internet des objets sont souvent filtrées afin que seules les données s'inscrivant en deçà ou au-delà de valeurs prédéfinies soient communiquées, à moins qu'elles ne soient communiquées que sous une forme reprenant l'intégralité des lectures à la fin d'un processus.

64. Un exemple classique d'utilisation par une chaîne de blocs des données recueillies via l'Internet des objets, est celle qui donne l'assurance de non-dépassement de températures données pour des marchandises sensibles à de tels changements (comme des fruits devant être conservés entre 4 et 15 °C pendant leur transport). Exemple : un appareil relié à l'Internet des objets et disposé à l'intérieur d'un conteneur a enregistré que des fruits ont été maintenus à une température de 0 °C pendant deux jours entiers durant leur transport. Cette information est transmise au contrat intelligent, qui informe la compagnie d'assurance du fait que l'exportateur doit être dédommagé des marchandises altérées par la température trop basse et qui exécute automatiquement le paiement sans que l'importateur ou l'exportateur ou la compagnie de transport ait besoin d'intervenir. Pour les compagnies d'assurance, cela permet de réduire sensiblement le coût de traitement des demandes d'indemnisation, car elles n'ont pas à recouper les informations fournies par l'expéditeur ou l'exportateur avec celles de la police d'assurance et à évaluer la véracité des demandes (les données de l'appareil relié à l'Internet des objets en fournissent la preuve), avant de demander le paiement. En outre, cela permet de réduire les coûts supportés par l'expéditeur ou l'exportateur, car ils n'ont pas besoin d'entreprendre d'autres démarches pour rassembler les justificatifs relatifs au problème survenu, et ils sont plus rapidement remboursés par la compagnie d'assurance.

E. La pertinence, selon le contexte, d'utiliser ou non la chaîne de blocs

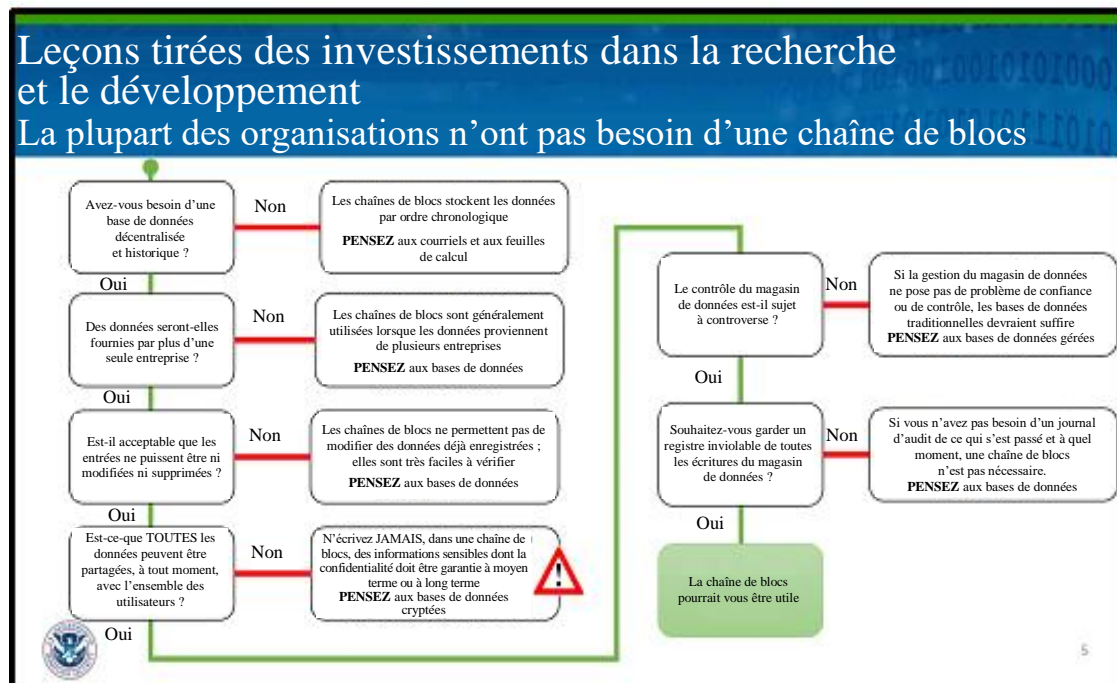
65. La décision d'utiliser une chaîne de blocs, que ce soit dans le secteur public ou le secteur privé, devrait être une décision commerciale fondée sur la capacité de la technologie à favoriser l'un des éléments suivants :

- Des services nouveaux et améliorés ;
- Des processus ou une mise en œuvre plus rapide(s) ; ou
- Des processus ou une mise en œuvre plus rentable(s).

66. Après avoir défini le processus métier pour lequel on envisage d'utiliser une chaîne de blocs, il peut être utile, à l'étape suivante de l'analyse, de se référer à l'arbre de décision du diagramme ci-dessous.

Figure 1

Quand utiliser la chaîne de blocs⁷



67. Si seule une des réponses fournies aux questions de la figure 1 est négative, il peut tout de même être justifié d'avoir recours à la chaîne de blocs, par exemple s'il est particulièrement important d'avoir un registre inviolable ou si ceux qui disposent d'un accès en lecture ne font pas confiance à ceux qui disposent d'un accès en écriture. En outre, dans certains cas, une base de données peut faire l'affaire, mais une chaîne de blocs peut s'avérer plus rapide ou moins coûteuse à mettre en œuvre ; il faut donc aussi prendre en compte les considérations de temps et de coût.

68. Il est important de se rappeler que l'utilisation de la chaîne de blocs implique un certain type d'authentification et que toutes les transactions n'exigent pas un niveau de fiabilité aussi élevé. Il est souligné dans la Loi type de la CNUDCI sur le commerce électronique de 1996 que la méthode d'authentification choisie devrait être « une méthode dont la fiabilité est suffisante au regard de l'objet pour lequel la communication électronique a été créée ou transmise, compte tenu de toutes les circonstances, y compris toute convention en la matière »⁸.

69. Le coût de calcul implicite de la technologie de la chaîne de blocs devrait également être pris en compte. Même lorsque cette technologie est proposée gratuitement, certaines dépenses interviendront plus tard dans la chaîne d'approvisionnement et pourront, en fonction de divers facteurs, augmenter le coût final supporté par l'utilisateur. Il convient donc d'analyser de près les avantages et les coûts. Il importe aussi de veiller à ce que l'utilisation de la technologie de la chaîne de blocs ne crée pas d'obstacles pour les micro,

⁷ Anil John, Directeur technique, Département de la sécurité intérieure des États-Unis, Direction des sciences et de la technologie, « Beyond Blockchain Basics », présentation donnée dans le cadre de la conférence annuelle sur les applications de sécurité informatique, 5 décembre 2018, https://www.acsac.org/2018/openconf/modules/request.php?module=oc_program&action=page.php&id=42 (consulté le 24 décembre 2018).

⁸ Voir aussi la recommandation n° 14 de la CEE sur l'authentification des documents commerciaux, disponible à l'adresse : https://www.unece.org/fileadmin/DAM/cefact/recommendations/rec14/ECE_TRADE_C_CEFAC2014_6F.pdf (consultée le 16 décembre 2016).

petites et moyennes entreprises, les économies en développement et les économies en transition.

70. Aujourd'hui, bien que de nombreuses entreprises aient conclu que la chaîne de blocs pourrait contribuer à améliorer certains processus de leur secteur, elles ne se sont pas engagées à la mettre en œuvre immédiatement, et restent pour l'instant dans une attitude attentiste. Sauf à pouvoir se servir d'une chaîne de blocs « prête à l'emploi », c'est probablement la meilleure approche à adopter dans les entreprises parce que la technologie est encore nouvelle et qu'elle n'a pas été mise à l'essai dans le cadre de nombreux processus. En outre, les entreprises veulent parfois mettre à l'essai la chaîne de blocs en interne afin d'acquérir de l'expérience et de déterminer tout changement de procédure ou de structure interne qu'il faudrait apporter avant de décider de rejoindre ou non l'une des nombreuses plateformes de chaînes de blocs qui sont en cours de développement et qui offrent des solutions « prêtes à l'emploi » ou promettent de le faire dans un avenir proche.

71. L'attentisme en la matière consiste généralement à mettre en œuvre un projet de démonstration de faisabilité et, si les résultats sont concluants, à examiner la manière dont un projet pilote plus vaste pourrait être mis en œuvre, avant de déployer l'application à l'échelle de l'entreprise.

72. Même si les résultats ne sont pas concluants, une démonstration de faisabilité peut aider une entreprise à mieux comprendre les applications possibles et les pièges de la chaîne de blocs, ce qui l'aidera à l'avenir à mieux évaluer si l'utilisation de cette technologie est pertinente dans d'autres domaines.

73. Dans le cas où, après avoir réalisé l'analyse ci-dessus, une entreprise décide de recourir à la démonstration de faisabilité et confirme ensuite son choix en faveur de cette technologie, l'étape suivante consistera à déterminer quelle chaîne de blocs utiliser. Toutes les chaînes de blocs ne se valent pas. Elles varient en fonction de la méthode de consensus, de la technique cryptographique, de la taille du réseau et du caractère privé de la chaîne de blocs ou de son accessibilité sur autorisation (voir les explications données plus haut). Il convient notamment d'examiner les points essentiels ci-après :

- **La vulnérabilité** au piratage informatique et aux autres défaillances du système ;
- **La robustesse**, c'est-à-dire la capacité du système à gérer les problèmes (code défectueux ou piratage, par exemple) ;
- **Le coût** de la transaction ;
- **La rapidité et la capacité d'expansion**, laissant entrevoir de gros volumes de transactions ; et
- **Le degré de protection de la vie privée** : absence totale d'anonymat, ou pseudo-anonymat ou anonymat total, et respect de la législation relative à la protection de la vie privée.

74. Afin d'évaluer ces caractéristiques, il faut avant tout déterminer les besoins et les préoccupations propres à une entreprise dans les domaines ci-dessus. C'est sur la base de ces besoins qu'une entreprise pourra envisager les différentes options existantes en termes de chaînes de blocs. Par exemple, assurer la traçabilité de concombres ou de diamants entraîne pour une entreprise un moins grand besoin de protection contre le piratage informatique (vulnérabilité) dans le premier cas que dans le second. Cela étant, les volumes de concombres en circulation sont probablement beaucoup plus importants que ceux des diamants, ce qui révèle l'importance de la scalabilité. La faible valeur des concombres renforce considérablement l'importance de se concentrer sur les coûts.

75. Enfin, il convient de s'appuyer sur des informations qui datent de moins de douze mois dans le cadre de cette dernière étape. Il s'agit d'un secteur en plein essor où de nombreuses personnes s'emploient à trouver des solutions pour résoudre des problèmes propres à tel ou tel modèle de chaînes de blocs. Par conséquent, ce qui était vrai il y a deux ans ou même dix-huit mois ne l'est peut-être plus aujourd'hui. Il peut également être très utile de consulter des programmeurs qui ont acquis de l'expérience dans l'application des chaînes de blocs, car il existe souvent des solutions de rechange aux différents problèmes, en particulier dans le cas des chaînes de blocs publiques, où la communauté d'experts est plus importante.

Annexe

<i>Secteur</i>	<i>Compléter uniquement si vous avez besoin de plus de détails que ce qui est indiqué dans le titre du chapitre</i>
Brève description	Une ou deux phrase(s), soit 240 caractères maximum
Organisme qui propose/exécute/met à l'essai	Si l'information n'est pas pertinente ou indisponible, indiquer « sans objet »
Contact pour tout complément d'information	Nom et adresse électronique (au minimum), éventuellement aussi : <ul style="list-style-type: none"> • Numéro de téléphone ; ou • Adresse postale ; ou • Site Web
Description longue	1 200 caractères maximum
Description des avantages commerciaux potentiels de l'utilisation de la chaîne de blocs	Devrait inclure uniquement les avantages découlant des caractéristiques particulières de la chaîne de blocs, c'est-à-dire ceux qui ne pourraient pas être obtenus à l'aide d'autres technologies
Préoccupations particulières (juridiques, techniques, etc.)	Il peut s'agir de la nécessité de réduire au minimum les temps de réponse, du besoin de reconnaissance juridique ou de la nécessité d'avoir un nombre minimum de membres du consortium ou de nœuds du réseau
Chaîne de blocs utilisée ou proposée	Bitcoin, Bitcoin Cash, Ethereum, chaîne de blocs gérée par consortium, chaîne de blocs privée, etc.
Type d'algorithme de consensus utilisé (si la chaîne de blocs est privée ou accessible sur autorisation ou gérée par un consortium)	Si l'information n'est pas pertinente ou indisponible, indiquer « s.o. »
Arguments pour ou contre et concessions à prendre en considération dans le choix d'une chaîne de blocs	Si l'information n'est pas pertinente ou indisponible, indiquer « s.o. »
Tout matériel spécial ou « autre » utilisé (Internet des objets, codes QR, etc.)	Si l'information n'est pas pertinente ou indisponible, indiquer « s.o. »
Tout logiciel libre utilisé ou proposé	Si l'information n'est pas pertinente ou indisponible, indiquer « s.o. »
Liens vers des informations connexes, y compris des Livres blancs techniques	Si l'information n'est pas pertinente ou indisponible, indiquer « s.o. »