Nations Unies ECE/TRADE/C/CEFACT/2022/12*

Conseil économique et social

Distr. générale
21 juillet 2022
Français
Original : anglais

Commission économique pour l'Europe

Comité exécutif

Centre des Nations Unies pour la facilitation du commerce et les transactions électroniques

Vingt-huitième session
Genève, 10 et 11 (matin) octobre 2022
Point 5 d) de l'ordre du jour provisoire
Recommandations et normes :
Documents d'aide à l'application

Rapport sur les travaux du domaine Gestion des données électroniques sur le rôle de l'Internet des objets dans la facilitation du commerce : guide sur les technologies, les communications et la connectivité de l'Internet des objets

Document présenté par le Bureau

Résumé

L'Internet des objets (IoT), grâce aux données qu'il génère, devient progressivement un élément à part entière de la gestion des entreprises et de la chaîne d'approvisionnement, et donc un outil essentiel au commerce. Pour aider les acteurs du commerce à mieux comprendre à la fois le fonctionnement des systèmes reposant sur les technologies de l'IoT (systèmes IoT) et la manière dont ces systèmes peuvent appuyer la facilitation du commerce et la gestion des infrastructures publiques, le CEFACT-ONU a élaboré le présent guide sur le rôle que l'IoT peut jouer à cet égard, dans lequel il donne un aperçu des technologies mises en œuvre dans l'IoT s'agissant des applications liées au commerce, l'objectif étant de fournir des explications claires aux personnes chargées de la mise en œuvre des technologies de l'information.

Publié sous la cote ECE/TRADE/C/CEFACT/2022/12, le présent document est soumis par le Bureau du CEFACT-ONU à la vingt-huitième session pour qu'il en soit pris note.

* Nouveau tirage pour raisons techniques (31 août 2022).

I. Introduction

1. L'Internet des objets (IoT) n'est plus un terme employé exclusivement par les experts. Il devient progressivement un élément à part entière de la gestion des entreprises et de la chaîne d'approvisionnement, car il génère des données qui facilitent la gestion des stocks, la maintenance du parc d'outillage, la gestion des bâtiments, la gestion des déclarations de sinistre et le suivi et la traçabilité d'actifs très divers. C'est pourquoi il est également devenu un outil essentiel au commerce.

2. L'IoT facilite la réflexion des particuliers et des entreprises et les aide à prendre des décisions plus judicieuses. Les dépenses liées aux technologies de l'IoT, qui ont atteint 742 milliards de dollars des États-Unis en 2020 et devraient dépasser les 1 000 milliards de dollars d'ici à 2023[1], témoignent de l'utilité et de l'utilisation croissante des écosystèmes IoT. La grande majorité d'entre elles sont effectuées par des entreprises qui cherchent à renforcer leur efficacité opérationnelle ou à trouver de nouvelles sources de revenus.

3. La facilitation du commerce se définit comme « la simplification, la normalisation et l'harmonisation des procédures et des flux d'informations y afférents, qui participent au mouvement des marchandises entre le vendeur et l'acheteur et au paiement de celles-ci »[2]. Les écosystèmes IoT peuvent faciliter le commerce en générant des données utilisables dans le cadre de procédures simplifiées. Par exemple, grâce aux données de statut et de localisation, il est possible de réduire le nombre d'inspections et de vérifications manuelles, et ces données peuvent également être utilisées en complément (voire, à terme, en remplacement) des certificats d'origine. Les données relatives à la localisation et aux conditions de transport des marchandises collectées par l'IoT peuvent servir à simplifier l'ensemble des déclarations de sinistres, que ce soit en lien avec des retards de livraison ou des marchandises endommagées (du fait de la température, de l'humidité, de secousses, etc.), et également à faciliter les opérations de rapprochement comptable (par exemple, entre les bons de commande et les bons de livraison), y compris pour les paiements par lettre de crédit.

4. Pour aider les acteurs du commerce à mieux comprendre à la fois le fonctionnement des systèmes reposant sur les technologies de l'IoT (systèmes IoT) et la manière dont ces systèmes peuvent faciliter le commerce et la gestion des infrastructures intergouvernementales, le Centre des Nations Unies pour la facilitation du commerce et les transactions électroniques (CEFACT-ONU) a élaboré les documents suivants :

- « Le rôle de l'Internet des objets dans la facilitation du commerce : l'Internet des objets dans les chaînes d'approvisionnement et les services publics », qui porte sur la manière dont l'IoT peut faciliter le commerce, ainsi que sur certaines des difficultés juridiques que rencontrent les opérateurs des systèmes IoT dans le secteur du commerce[3] ;
- Le présent document, qui donne une vue d'ensemble des technologies de l'IoT utilisées dans les applications liées au commerce, l'objectif étant de fournir des explications claires aux personnes qui, en tant que gestionnaires, maîtrisent les technologies de l'information, mais qui n'ont au mieux qu'une expérience limitée de l'IoT ;
- Le « Livre blanc sur les normes de l'Internet des objets au service de la facilitation du commerce »[4], dans lequel le CEFACT-ONU examine la nécessité d'adopter de nouvelles normes pour promouvoir l'utilisation de l'IoT dans le commerce ;

[1] Statista, « Prognosis of worldwide spending on the Internet of Things (IoT) from 2018 to 2023 », 28 juin 2022, disponible à l'adresse https://www.statista.com/statistics/668996/worldwide-expenditures-for-the-internet-of-things/ (page consultée le 26 janvier 2021).

[2] Le Guide pratique relatif à la facilitation du commerce est disponible à l'adresse https://tfig.unece.org/FR/details.html.

[3] CEFACT-ONU, « Rapport du domaine Gestion des données électroniques sur le rôle de l'Internet des objets dans la facilitation du commerce : l'Internet des objets dans les chaînes d'approvisionnement et les services publics » (ECE/TRADE/C/CEFACT/2022/11), 2022.

[4] CEFACT-ONU, « Livre blanc sur les normes de l'Internet des objets au service de la facilitation du commerce » (ECE/TRADE/C/CEFACT/2022/9), 2022.

- Le « Livre blanc de facilitation du commerce sur les Conteneurs intelligents »[5], dans lequel le CEFACT-ONU analyse en profondeur l'utilisation de l'IoT dans le secteur des transports.

5. La facilitation du commerce passe par l'échange de données entre les différents acteurs. Or, les données générées par l'IoT sont très difficilement exploitables lorsqu'elles reposent sur des définitions et des formats divergents, car il faut alors procéder à un fastidieux travail de retraitement. Par conséquent, si l'on veut tirer pleinement parti du potentiel de l'IoT au service de la facilitation du commerce, il faut normaliser les données générées à l'aide des technologies mises en œuvre. Le CEFACT-ONU peut apporter des solutions à ce problème grâce à sa bibliothèque de composants communs, qui contient des définitions de données et des listes de codes. Il lui reste cependant encore à parvenir à faire connaître l'existence de cette bibliothèque aux développeurs de systèmes IoT, à mettre à leur disposition des informations faciles d'accès sur son utilisation, et à veiller à ce qu'ils puissent trouver les données dont ils ont besoin. Le projet du CEFACT-ONU sur les conteneurs intelligents a grandement contribué à faire en sorte que les données requises soient disponibles, mais il faudra déployer des efforts supplémentaires pour que les données générées par l'IoT puissent être pleinement utilisées dans d'autres domaines tels que la gestion des stocks, la comptabilité et la finance.

6. Pour une analyse plus approfondie des normes existantes et du besoin éventuel d'en adopter de nouvelles pour promouvoir l'utilisation de l'IoT aux fins de la facilitation du commerce, on pourra se référer au rapport susmentionné du CEFACT-ONU sur le rôle de l'Internet des objets dans les chaînes d'approvisionnement et les services publics.

II. Aperçu des technologies de l'IoT

7. Qu'est-ce que l'Internet des objets ? Un système IoT est un réseau de réseaux dans lequel, d'une façon générale, un nombre important d'objets, de capteurs ou de dispositifs interconnectés à l'aide d'une infrastructure de communication et d'information permettent de fournir des services à valeur ajoutée grâce à une gestion et un traitement intelligents des données utilisées à différentes fins (par exemple, les villes intelligentes, la santé intelligente, les réseaux électriques intelligents, les maisons intelligentes, les transports intelligents et les achats intelligents).

8. Pour faire partie de l'IoT, les « objets » mentionnés ci-dessus (ci-après dénommés « dispositifs ») doivent être dotés d'un identifiant unique et avoir la capacité de transférer des données sur un réseau sans intervention humaine, que ce soit entre personnes ou avec un ordinateur[6].

9. Les dispositifs IoT peuvent :

- Être munis d'un ou de plusieurs capteurs (de température, d'humidité, de mouvement, etc.) ;
- Transmettre des informations sur leur emplacement (à l'aide de calculs ou en utilisant le système GPS) ;
- Transmettre ou recevoir des instructions (par exemple, l'envoi de signaux à un conteneur de transport réfrigéré afin d'en ajuster la température) ;
- Être dotés d'une certaine capacité de traitement (par exemple, analyser les données fournies par des capteurs et envoyer des alertes en cas de dépassement des valeurs attendues) ;

[5] CEFACT-ONU, *Livre blanc de facilitation du commerce sur les Conteneurs intelligents – l'exploitation en temps réel des données de conteneurs intelligents pour parvenir à l'excellence dans la chaîne d'approvisionnement* (ECE/TRADE/446), 2020. Accessible à l'adresse https://unece.org/DAM/trade/Publications/ECE_TRADE_446F_SmartContainers.pdf.

[6] Alexander S. Gillis, « What is the internet of things (IoT)? »,TechTarget, mars 2022. Disponible à l'adresse https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT (page consultée le 17 juillet 2022)

- Collecter des données issues d'autres dispositifs IoT pour les transmettre ou procéder à une première analyse (les dispositifs capables d'analyser des données sont appelés « dispositifs informatiques en périphérie de réseau ») ;
- Être fixés sur une entité vivante telle qu'un animal (aux fins, par exemple, du suivi de la santé des animaux pendant leur transport).

10. Les types de données collectées par les dispositifs IoT sont les suivants :

- *Données d'état* : il s'agit des données IoT les plus simples, qui servent principalement à alimenter des analyses complexes, mais qui peuvent aussi avoir une valeur propre importante. Dans le commerce, ces données sont souvent fournies par des capteurs placés dans les conteneurs, qui donnent des informations sur la température et le taux d'humidité ;
- *Données de localisation* : il s'agit de données qui permettent de déterminer l'emplacement ou la position d'un objet présentant un intérêt. Le commerce international utilise de nombreux dispositifs IoT pour suivre la position des camions, des conteneurs et des produits ;
- *Données d'automatisation* : il s'agit de données fournies par les capteurs qui participent au contrôle de processus et remplissent des fonctions telles que le contrôle et le réglage des systèmes de chauffage, d'éclairage et de gestion des conditions de stockage ;
- *Données exploitables* : il s'agit de données qui, après analyse, servent notamment à repérer des emplacements de stationnement ou de stockage disponibles, à réduire la surconsommation d'énergie (par exemple, grâce à des capteurs qui mesurent la profondeur de l'eau, les courants et le vent afin qu'un navire puisse adapter sa vitesse pour consommer moins de carburant), à améliorer l'entretien préventif des équipements (par exemple, les camions ou les chariots élévateurs), ainsi que la performance et le suivi des systèmes pendant toute la durée de vie d'un navire ;
- *Données de rétroaction* : l'IoT peut également permettre de créer des boucles de rétroaction servant à évaluer les processus de manutention et de transport des marchandises et à apporter les changements nécessaires.

11. Les données collectées ou générées par un écosystème IoT peuvent être transmises directement à une application (dans le cloud ou une chaîne de blocs, ou sur un serveur privé) ou être entièrement ou partiellement analysées au niveau local avant leur transmission. Dans le cas des écosystèmes IoT qui génèrent de grands volumes de données, les applications sont souvent situées dans le cloud, et des processus d'intelligence artificielle sont mis en œuvre pour l'analyse des données.

12. Les applications qui utilisent l'IoT reposent souvent sur des dispositifs déployés en réseau (écosystèmes). Par exemple, l'écosystème IoT d'un navire intelligent lui fournit des informations sur son environnement (vent, courants, etc.) ainsi que sur sa cargaison, ses équipements et son fonctionnement, ce qui réduit (voire supprime) la nécessité de la présence d'un équipage. Dans le même ordre d'idées, l'écosystème IoT d'un entrepôt intelligent assure le suivi de différents paramètres relatifs au bâtiment et contrôle les équipements afin que la température et le taux d'humidité se maintiennent dans une plage prédéfinie, pour minimiser les coûts, et des messages d'alerte sont envoyés en cas de problème.

III. Dispositifs et technologies de l'IoT

13. Pour fonctionner efficacement, les dispositifs IoT doivent satisfaire à diverses prescriptions, certaines liées aux dispositifs eux-mêmes et d'autres aux écosystèmes IoT dans lesquels ils fonctionnent. Les principales prescriptions auxquelles ils doivent répondre sont les suivantes :

- Être dotés de capteurs et/ou d'émetteurs et/ou de récepteurs ;
- Être petits, peu coûteux et consommer peu ou pas d'énergie (pour que la pile qui les alimente puisse durer longtemps) ;

- Posséder un identifiant unique et pouvoir être géolocalisés ;
- Transmettre des données soit sur de courtes distances vers d'autres dispositifs IoT, soit sur des distances moyennes à longues ;
- Communiquer et partager des données avec d'autres systèmes (ce qui nécessite une interopérabilité) ;
- Faire l'objet d'une maintenance des éléments matériels comme logiciels ;
- Être sécurisés et protégés contre les accès non autorisés et la falsification des données ;
- Fonctionner dans le respect de la réglementation en vigueur.

14. Les nouvelles technologies qui sont mises au point chaque semaine, voire chaque jour, peuvent avoir des incidences sur les nouvelles prescriptions en matière d'IoT. Dans la présente section, nous tenterons d'examiner plus en détail les prescriptions décrites précédemment et les technologies connexes − à l'exception des questions juridiques, qui sont examinées dans le rapport portant sur l'Internet des objets dans les chaînes d'approvisionnement et les services publics.

A. Types de dispositifs IoT

15. Il existe de nombreux types de dispositifs IoT. On trouvera ci-après une présentation des principaux, à savoir les dispositifs avec capteurs, les dispositifs sans capteurs, les dispositifs informatiques en périphérie de réseau et les passerelles IoT.

1. Dispositifs IoT dotés d'un ou de plusieurs capteurs ou actionneurs

16. En dotant les dispositifs IoT de technologies de détection, il est possible de générer des informations qui décrivent une caractéristique du monde réel. Les capteurs collectent des informations qui sont traitées dans un écosystème IoT, à un ou plusieurs niveaux. Par exemple, le dispositif de collecte peut déterminer si une température se situe dans la plage attendue ou la transmettre à un dispositif informatique en périphérie de réseau pour prise de décisions. Ensuite, seules les données de température hors limites sont transférées vers un autre dispositif informatique pour analyse et traitement complémentaires.

17. La variété et le nombre grandissants de capteurs qui peuvent être inclus dans de petits dispositifs IoT tiennent aux avancées de la nanotechnologie, en particulier des systèmes microélectromécaniques. Il s'agit de machines miniatures comportant des composants électroniques et mécaniques tels que des ressorts, des canaux, des cavités, des trous et des membranes. Leur taille varie de plusieurs millimètres à moins d'un micromètre (c'est-à-dire beaucoup moins que l'épaisseur d'un cheveu).

18. Du point de vue de l'IoT, les systèmes microélectromécaniques les plus intéressants sont les capteurs (pour détecter un état) et les actionneurs (pour contrôler un processus). Les microcapteurs existent pour une multitude de tâches, notamment la détection de la température, de la pression, de l'humidité, du mouvement, de produits chimiques ou de gaz, de champs magnétiques, de rayonnements, etc. Il existe également différents types de microactionneurs, notamment les microsoupapes et les pompes servant à contrôler les flux de gaz et de liquides, les commutateurs optiques et les miroirs servant à rediriger ou à moduler les faisceaux lumineux, et les microvolets utilisés pour moduler les flux d'air sur les aérofreins.

19. Les progrès des systèmes microélectromécaniques dépendent de l'évolution des techniques de microfabrication (notamment de la possibilité de les incorporer dans des circuits intégrés), ainsi que de la qualité de leur conception. Les systèmes microélectromécaniques sont également appelés micromachines, dispositifs micro-usinés ou microsystèmes technologiques[7].

[7] Voir la définition données sur le site de TechTarget, à l'adresse https://internetofthingsagenda.techtarget.com/definition/micro-electromechanical-systems-MEMS. Pour plus d'informations sur les systèmes microélectromécaniques, se référer au site Web de la

2. Dispositifs IoT sans capteurs

20. Certains dispositifs IoT ne sont pas dotés de capteurs et ne servent qu'à recevoir ou à transmettre de l'information. Par exemple, un récepteur peut être un actionneur qui reçoit des instructions à distance pour le verrouillage ou le déverrouillage d'une porte ou le démarrage d'une machine. Ce second type de dispositif IoT peut être passif ou actif et est doté d'étiquettes d'identification par radiofréquence (RFID) et de communication en champ proche (CCP) qui permettent à d'autres dispositifs IoT de lire des informations.

3. Dispositifs informatiques en périphérie de réseau

21. Les dispositifs informatiques en périphérie de réseau collectent des données provenant d'autres dispositifs IoT et présentent certaines caractéristiques (voir ci-après) permettant de réduire les coûts afférents aux systèmes IoT. Il s'agit notamment des caractéristiques suivantes :

- Une **réduction du coût des dispositifs**, obtenue en confiant les coûteuses tâches de calcul analytique à d'autres appareils que les dispositifs IoT individuels, et en dotant ces derniers uniquement de capacités de transmission à courte portée ;
- Une **réduction des coûts de transmission des données**, obtenue en ne transmettant, après analyse, que les données qui répondent à des critères définis ;
- Une **diminution du temps de latence** : les calculs étant effectués au plus près de la source de données, le temps de transfert est réduit, ce qui présente un intérêt pour les processus de fabrication et les applications médicales, dans lesquels la rétroaction en temps réel et la rapidité de réponse jouent un rôle essentiel ;
- Un **renforcement de la confidentialité des données** : le calcul en périphérie de réseau offre davantage de possibilités de traitement des données. Par exemple, il est possible de résoudre certains problèmes liés à la protection des données en traitant les données personnelles au niveau local et en ne transmettant que des résultats anonymes à des fins de traitement ultérieur et de stockage ;
- Une **sécurité accrue** : les architectures centralisées sont vulnérables aux attaques par déni de service distribué. Grâce à l'architecture informatique décentralisée en périphérie de réseau, le système dans son ensemble ne peut être bloqué du fait d'une perturbation isolée ;
- **Évolutivité** : l'architecture informatique en périphérie de réseau facilite un développement souple des ressources informatiques, à mesure que de nouveaux dispositifs sont ajoutés à un système IoT, car elle évite de faire peser sur un système central le poids des calculs et de la transmission et du stockage des données. Par exemple, un dispositif informatique en périphérie de réseau peut analyser les résultats de nombreux capteurs en temps réel et ne transmettre que les moyennes calculées sur des périodes déterminées et/ou les relevés qui se situent en dehors d'une plage prédéfinie ;
- Une **diminution des coûts de maintenance et de l'impact environnemental** : les dispositifs IoT, s'ils sont associés à des capteurs simples et si les fonctions de calcul sont déportées vers des dispositifs informatiques en périphérie de réseau, ne nécessitent que peu de puissance de calcul, ce qui prolonge la durée de vie des piles. Cela permet de réduire la fréquence des entretiens et de limiter la production de déchets.

4. Passerelles IoT

22. Une passerelle IoT est un dispositif informatique en périphérie de réseau dédié à la transmission de données. Ces passerelles servent à réduire le coût des télécommunications : elles reçoivent des communications longue distance et les renvoient sur des dispositifs IoT moins coûteux ayant des besoins énergétiques moindres et des capacités de communication

société MEMS and Nanotechnology Exchange, à l'adresse https://www.mems-exchange.org/MEMS/what-is.html (page consultée le 18 juillet 2022).

à courte distance (par exemple, en Bluetooth), et elles collectent les données fournies par ces dispositifs pour les retransmettre à des serveurs distants.

B. Besoins énergétiques de l'IoT

23. L'une des principales difficultés concrètes que pose la mise en œuvre d'un réseau IoT est la consommation d'énergie électrique. De nombreux composants IoT (notamment ceux qui sont utilisés dans les transports) doivent être relativement simples et capables de fonctionner pendant de longues périodes, sans surveillance et dans des endroits éloignés. Il faut donc qu'ils soient économes en énergie, qu'ils soient dotés de piles longue durée et que des stratégies soient mises en œuvre pour maintenir l'intégrité des signaux (communications).

24. Ces exigences se traduisent par un certain nombre de contraintes de conception, qui varient selon l'utilisation prévue du dispositif et le mode de communication utilisé pour la transmission des données. Par exemple, dans le cas d'un dispositif IoT doté d'une radio sans fil, la meilleure façon d'économiser l'énergie est de s'assurer que la radio n'est alimentée qu'au moment de son utilisation. De même, dans le cas des canaux cellulaires, il convient de choisir un protocole de communication efficace et sécurisé qui nécessite un temps système minimal. Dans la plupart des cas, il existe des émetteurs à faible consommation d'énergie grâce auxquels les appareils peuvent se mettre en veille et ne s'activer que lorsqu'un événement se produit, ou bien être programmés pour se « réveiller » lorsque des paramètres doivent être mesurés.

25. Malgré l'existence de technologies permettant une faible consommation d'énergie, les déploiements à grande échelle de systèmes IoT comprenant des milliers de dispositifs peuvent toujours poser de sérieux défis de maintenance liés à la gestion énergétique, par exemple la nécessité de détecter les dispositifs qui tombent en panne ou dont les piles sont épuisées et de prendre des mesures correctrices[8], ou la probabilité que beaucoup de ces dispositifs déployés en grand nombre doivent être remplacés dans un court laps de temps à la fin de leur durée de vie. Par exemple, si 10 000 dispositifs ayant une autonomie de trois ans sont utilisés pendant deux ans, 5 000 devront être remplacés au cours des quatrième et cinquième années.

C. Localisation des dispositifs et des objets cibles

26. Les besoins de géolocalisation d'un dispositif sont déterminés par l'application ou l'écosystème IoT. Si un dispositif IoT est relativement immobile (par exemple, un capteur dans un feu de circulation ou une puce RFID installée à un endroit fixe dans un entrepôt), ce n'est qu'au moment de son installation ou de son déplacement qu'il est nécessaire de transmettre des informations sur sa localisation (ou bien celle-ci peut être enregistrée par l'installateur, ce qui supprime le besoin de transmission). En revanche, si le dispositif IoT est fixé sur un bien qui fait l'objet d'un suivi, comme un colis ou un conteneur, il se peut que son emplacement doive être transmis plusieurs fois par jour, voire encore plus fréquemment. La plupart des dispositifs IoT étant de faible puissance, il existe une corrélation entre d'une part, la puissance requise pour déterminer l'emplacement et transmettre l'information, et d'autre part le coût du dispositif et la fréquence des opérations de maintenance.

27. Si la connaissance de l'emplacement approximatif des dispositifs IoT suffit (par exemple, pour savoir si un article a transité par un quai de chargement ou s'il se trouve dans un bâtiment ou un site identifié), une passerelle IoT capable de détecter la présence de dispositifs simples et passifs (tels que des étiquettes RFID) peut permettre de fournir des informations de localisation suffisantes.

28. Des émetteurs-récepteurs à signal radio permettent de fournir des informations de localisation plus précises. Plus leur portée est courte, moins ils sont énergivores. C'est pourquoi le GPS est l'une des solutions les plus coûteuses. Pour minimiser ces coûts, il est possible d'utiliser des dispositifs à faible consommation d'énergie en conjonction avec un

[8] La majorité des dispositifs IoT sont étanches, ce qui rend nécessaire le remplacement lorsque leurs piles sont épuisées, car il est impossible de changer ces dernières.

dispositif informatique en périphérie de réseau plus puissant. Ce dispositif doit ensuite : 1) obtenir les identifiants des dispositifs moins puissants placés suffisamment près de lui pour qu'une transmission à faible consommation énergétique puisse se faire (et, si nécessaire, déterminer leur position exacte) ; 2) recevoir un signal GPS et l'utiliser pour déterminer l'emplacement des autres dispositifs de faible puissance ; 3) transmettre la ou les positions des dispositifs de faible puissance, accompagnées de leurs identifiants (peut-être par satellite). Ces dispositifs d'informatique en périphérie de réseau peuvent être installés sur des véhicules (par exemple, des camions) ou des navires pour recueillir des informations sur l'emplacement des colis ou des conteneurs transportés.

29. Les GPS et les dispositifs de signalisation enregistrés sont les principaux moyens de déterminer la localisation d'un objet à l'aide de signaux radio. Un système GPS consiste en un récepteur qui utilise les signaux radio émis par différents satellites pour calculer sa position.

30. Les dispositifs de signalisation enregistrés servent à déterminer (grâce à une base de données en ligne[9]) ou à calculer (sur la base d'une méthode appelée triangulation ou trilatération[10]) l'emplacement du récepteur de signaux radio placé dans un dispositif IoT. Les étapes précises à suivre varient en fonction de la source des signaux (point d'accès Wi-Fi, point d'accès Bluetooth ou relais cellulaire).

31. Une fois que l'emplacement d'un dispositif IoT a été déterminé, il peut être nécessaire de transmettre la position d'autres objets cibles (par exemple, des palettes dans un entrepôt). Si le dispositif est fixé sur un objet cible tel qu'un conteneur, cette opération est relativement simple, mais le fait d'apposer un dispositif IoT sur chaque objet cible peut s'avérer coûteux au regard de la valeur de l'objet ; dans certains cas, cela peut même être impossible à réaliser.

32. Dans ce cas, il existe deux moyens d'associer des objets cibles à un dispositif IoT :

- Le récepteur de signaux radio intégré dans le dispositif IoT lit les informations d'identification relatives aux objets cibles, tels que les identifiants RFID[11] ou les étiquettes CCP[12] ;
- Les caractéristiques d'identification individuelles d'un objet sont obtenues au moyen d'une analyse d'image (ce qui nécessite que le dispositif IoT ou le dispositif informatique en périphérie de réseau dispose de capacités de calcul avancées, et donc plus coûteuses).

IV. Communications et connectivité

33. Il est essentiel que le transfert des données s'opère entre les couches IoT qui collectent des informations sur les paramètres physiques (par exemple, l'emplacement, la température ou la composition chimique) et les couches cybernétiques qui agrègent ces informations et effectuent divers calculs et processus analytiques. Cependant, la capacité à transmettre des données engendre des coûts supplémentaires, tant pour le dispositif IoT que pour la communication en elle-même. En outre, l'efficacité et la sécurité de la transmission dépendent des choix technologiques qui ont été retenus (voir ci-après).

[9] Voir https://cellidfinder.com/articles/how-to-find-cellid-location-with-mcc-mnc-lac-i-cellid-cid.

[10] Pour plus d'informations sur les techniques de trilatération, voir Ana Roxin, Jaafar Gaber, Maxime Wack et Ahmed Nait Sidi Moh, « Survey of Wireless Geolocation Techniques », IEEE Global Communications Conference 2007, novembre 2007, Washington, ffhal-00701118f, disponible à l'adresse https://hal.archives-ouvertes.fr/hal-00701118/document.

[11] Pour plus d'informations sur le fonctionnement du système RFID, voir https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid.htm (page consultée le 18 juillet 2022).

[12] Les étiquettes CCP ne peuvent être lues qu'à une distance inférieure ou égale à 4 cm, mais elles sont hautement sécurisées. Pour plus d'informations, voir https://nfc-forum.org/what-is-nfc/about-the-technology/ (page consultée le 18 juillet 2022).

A. Communications

1. Communications − technologie sans fil

34. La plupart des communications entre les dispositifs d'un système IoT sont fondées sur la technologie sans fil, et les deux types de réseaux les plus fréquemment utilisés sont les suivants :

- **Bande de fréquences à 2,4 GHz** : cette bande, destinée à la transmission à courte ou moyenne portée et facile à mettre en œuvre, convient pour les smartphones et les passerelles IoT. Il peut s'agir par exemple des normes Wi-Fi, Bluetooth ou Zigbee. Cette méthode de communication est la plus pratique, car il n'est généralement pas nécessaire de disposer d'une licence, ce qui facilite le déploiement à l'échelle mondiale.
- **Bande de fréquences à 920 MHz** : cette bande permet une transmission à moyenne ou longue portée, par exemple à l'aide des technologies EnOcean, Z-Wave ou Wi-SUN et des réseaux LPWA[13] (Low-Power Wide Area) (c'est-à-dire LoRaWAN, Sigfox, NB-IoT). Une licence radio n'est pas nécessaire dans de nombreux pays, mais les largeurs de bande disponibles varient, de sorte qu'il est difficile de mettre en œuvre des applications au niveau mondial[14].

2. Communications − formats/normes (protocoles)

35. Le Wi-Fi est le seul moyen de communication sans fil régi par le protocole TCP/IP[15] qui soit utilisé dans les systèmes IoT. C'est pourquoi les passerelles IoT, qui collectent les informations provenant des dispositifs IoT situés à proximité, doivent souvent convertir dans un format compatible TCP les données reçues afin qu'elles puissent être transmises par Internet.

36. Les principaux protocoles utilisés dans l'IoT sont le HTTP et le MQTT, suivis par l'UDP :

- **HTTP** : à l'origine, il s'agit d'un protocole de communication servant à envoyer et à recevoir du contenu tel que du HTML. C'est un protocole très simple et polyvalent, raison pour laquelle il est souvent utilisé dans l'IoT. Cependant, il requiert qu'un en-tête de message soit joint aux demandes et aux réponses. D'autres solutions sont donc utilisées lorsque les volumes de données sont importants, afin de minimiser les coûts de transmission.
- **MQTT** : ce protocole de livraison de données permet d'alléger les messages, et il comprend également une spécification, appelée QoS, qui permet de préciser un niveau de garantie de livraison.
- **UDP** : ce protocole est le plus léger, mais il ne garantit pas la fiabilité, l'ordre ou l'intégrité des données. Il n'est donc utilisé que pour le transfert de données (c'est-à-dire pas pour la transmission d'instructions ou de codes), et uniquement lorsqu'une confirmation de la livraison n'est pas requise.

37. En plus de créer une compatibilité de transmission avec les protocoles Internet, les passerelles IoT peuvent également crypter les données afin de les protéger sur les réseaux et pendant leur transmission. Dans ce contexte, les passerelles peuvent être considérées comme une couche supplémentaire entre le cloud et les dispositifs IoT, capable de filtrer les attaques et les tentatives illégales d'accès au réseau.

[13] Pour plus d'informations sur les réseaux LPWA, voir https://www.paessler.com/it-explained/lpwa (page consultée le 18 juillet 2022).

[14] Pour plus d'informations sur les types de fréquences, voir http://www.ginsei-jp.com/920MHz_vs_24.html. Pour plus d'informations sur la technologie LoRaWAN, voir https://www.emnify.com/iot-glossary/lorawan (page consultée le 18 juillet 2022).

[15] Les règles qui régissent le fonctionnement de l'Internet, communément appelées « protocole TCP/IP », permettent aux ordinateurs de communiquer entre eux.

B. Connectivité

1. Connectivité − technologies de réseau

38. Un réseau virtuel est constitué de matériels et de logiciels qui ne sont pas physiquement connectés, mais qui communiquent entre eux selon un ensemble de normes et de règles, généralement par Internet. Lors de l'élaboration d'un réseau virtuel IoT (écosystème), les caractéristiques importantes à prendre en compte sont la signalisation, la détection de présence, la bande passante, le canal de communication et la sécurité.

39. Au vu de la demande croissante de réduction du temps de latence (délai entre la transmission et la réception) et de renforcement de la sécurité, les normes de réseau virtuel jouent désormais un rôle prépondérant dans les systèmes IoT.

40. Par exemple, les **réseaux étendus gérés par logiciel** (**SD-WAN**[16]) sont souvent utilisés dans le secteur des télécommunications, car ils offrent des bandes passantes élevées et un débit rapide, ainsi que la possibilité d'offrir des services à moindre coût. En outre, des technologies de réseau virtuel encore plus rapides, telles que celles qui utilisent des réseaux maillés, commencent à faire leur apparition. Les **réseaux maillés**[17] permettent à n'importe quel nœud individuel de communiquer directement, au moyen de communications cryptées de pair à pair (P2P), avec chaque autre nœud ou avec des nœuds individuels sur le même segment de réseau, d'une manière rapide et fiable, semblable à celle d'un réseau local (LAN), mais sur presque n'importe quelle distance.

41. Une autre technologie de réseau importante, souvent utilisée dans l'IoT, est celle des **réseaux étendus à faible puissance** (LPWAN)[18]. De nombreuses applications IoT doivent transmettre des données sur de longues distances et pendant de longues périodes, parfois des années. Il s'agit par exemple de capteurs agricoles, de capteurs situés dans des entrepôts ou dans des villes, utilisés par exemple pour la collecte des ordures, l'éclairage ou le stationnement. Revers de la médaille, les transmissions faites sur les réseaux LPWAN peuvent ne pas aboutir en raison d'interférences, de sorte que ces réseaux ne peuvent pas être utilisés pour des applications d'importance critique, comme dans le domaine des soins de santé ou des processus industriels. Toutefois, l'impact est négligeable si les données transmises par un capteur d'irrigation ou un capteur placé dans une poubelle arrivent avec un peu de retard.

42. Soulignant l'importance de la connectivité et des normes établies pour appuyer l'utilisation de l'IoT dans le commerce, la Digital Container Shipping Association (DCSA) a publié des normes de connectivité applicables aux passerelles IoT, qui sont entièrement compatibles avec les normes d'interopérabilité du CEFACT-ONU[19].

43. Chaque moyen de connectivité IoT présente ses propres avantages et inconvénients liés à la transmission de données (par exemple, la quantité de données et la fréquence de transmission), au temps de latence, à la consommation d'énergie, au coût et à la sécurité, pour n'en citer que quelques-uns. Les transferts rapides de grandes quantités de données consomment généralement plus d'énergie. En contrepartie d'une faible consommation énergétique, la portée est généralement plus courte, et la bande passante plus étroite.

44. Le choix du système le mieux adapté dépendra de l'objectif visé : un organisme chargé de faire des relevés de compteurs dans une ville ou une grande installation comme un port pourrait envisager d'utiliser la technologie LoRa[20], qui permet d'envoyer de petites quantités de données à intervalles réguliers. Dans un environnement industriel comportant des millions

[16] Pour plus d'informations sur l'approche SD-WAN, voir https://www.networkworld.com/article/3031279/sd-wan-what-it-is-and-why-you-ll-use-it-one-day.html (page consultée le 18 juillet 2022).

[17] Pour plus d'informations sur les réseaux maillés, voir https://computer.howstuffworks.com/how-wireless-mesh-networks-work.htm (page consultée le 18 juillet 2022).

[18] Pour plus d'informations sur les réseaux LPWAN, voir https://www.iotforall.com/what-is-lpwan-lorawan.

[19] Voir le site Web de la DSCA https://dcsa.org/standards/iot-connectivity.

[20] La technologie LoRa (abréviation de « long range ») repose sur une technique de modulation par étalement du spectre dérivée de la technologie CSS (chirp spread spectrum). Pour plus d'informations, voir https://www.semtech.com/lora/what-is-lora.

de petits capteurs en temps réel, qui nécessite une connectivité ultra fiable et à faible temps de latence, la 5G pourrait être la solution la plus adaptée. Quant aux entreprises agricoles qui veulent s'appuyer sur l'IoT, la technologie cellulaire ne convient pas, et un WAN de faible puissance à longue portée pourrait être la meilleure solution.

2. Connectivité − flux de données

45. Le cœur de tout écosystème d'objets connectés est l'orchestration des flux de données, autrement dit l'acheminement des « ensembles de données » à destination et en provenance des dispositifs IoT, y compris les systèmes périphériques et les passerelles, l'informatique en nuage, les autres bases de données/chaînes de blocs et les applications logicielles d'exploitation et/ou d'analyse (y compris les systèmes d'intelligence artificielle), et les interactions entre ces ensembles de données. Pour mettre en place cette orchestration, il convient de prendre en compte les éléments suivants :

- **Interopérabilité** : Dans le contexte de l'IoT, cette notion désigne la capacité des systèmes ou des composants des systèmes à communiquer entre eux, indépendamment de leur fabricant ou de leurs spécifications techniques. Pourquoi l'interopérabilité est-elle nécessaire ? Imaginons, dans un immeuble de bureaux, un écosystème d'objets connectés dans lequel le système qui commande l'appareil de climatisation parle une langue différente de celle que parle le système qui commande les stores des fenêtres (tels qu'ils sont programmés par leurs fabricants). Dans ce cas, ces deux systèmes ne seraient pas en mesure de communiquer entre eux ou d'agir de manière coordonnée, ce qui entraînerait pour le propriétaire des factures d'électricité plus élevées que nécessaire. Étant donné que l'écosystème technologique n'en est qu'à ses débuts et que le marché des dispositifs IoT est fragmenté, l'interopérabilité est une question essentielle.
    - La norme IEEE P2413-2019[21], qui décrit un cadre d'architecture applicable à l'IoT, est un exemple de norme en matière d'interopérabilité. Cette description est axée sur les préoccupations partagées par les parties prenantes des systèmes d'objets connectés dans plusieurs domaines (transport, soins de santé, réseau intelligent, etc.), telles que les exigences de sécurité des communications par l'IoT.
    - Un autre exemple est la norme de la bibliothèque de composants communs de l'ONU[22], qui favorise l'**interopérabilité sémantique** en normalisant la définition des données. Ce niveau d'interopérabilité garantit que les données provenant de différents systèmes utilisent les mêmes définitions, par exemple pour la température ou l'heure ou pour des concepts plus abstraits tels que celui de « hors limites ».
    - L'interopérabilité au niveau du **format des données** nécessite souvent des conversions entre les normes et les formats de communication utilisés dans un réseau local d'objets connectés et ceux qui sont utilisés sur Internet. Dans la plupart des cas, ce processus est effectué sur des passerelles, mais il peut également être intégré dans les interfaces de programmation d'applications utilisées pour la communication d'instructions et de données entre les logiciels.
- Pour dégager des tendances, il faut envisager d'**agréger les données** présentant des caractéristiques définies et provenant de divers endroits. Cette agrégation peut avoir lieu soit sur une passerelle locale, soit dans un système central de données en nuage.
- Pour **transférer des données vers différents lieux et supports de stockage**, ce qui peut s'avérer nécessaire pour de multiples raisons, il faut procéder à une planification minutieuse afin d'assurer le suivi des différentes versions et de savoir quand les

[21] La norme IEEE P2413-2019 (*IEEE Standard for an Architectural Framework for the Internet of Things (IoT)*) est disponible à l'achat ou par abonnement à l'adresse suivante : https://standards.ieee.org/content/ieee-standards/en/standard/2413-2019.html.

[22] Guide explicatif du CEFACT-ONU sur les éléments de base des Nations Unies, 2017, disponible à l'adresse suivante : https://unece.org/fileadmin/DAM/cefactGuidanceMaterials/ExecutiveGuides/CCL-CCTS-ExecGuide_Fre.pdf.

données doivent être identiques à deux endroits différents (soit elles sont identiques, soit il est facile de déterminer qu'elles ne le sont pas) et pourquoi.

- **Modifications éventuelles des flux de données** : Les écosystèmes d'objets connectés doivent être conçus de manière flexible afin que les flux de données puissent être modifiés à tout moment pour tirer parti de nouvelles technologies, de nouvelles applications et de changements de fournisseurs de services.
- **Génération de données d'apprentissage pour l'intelligence artificielle (IA)** : L'IoT peut générer en continu des données qui seront utilisées par les systèmes d'IA à des fins d'apprentissage et de mise au point de modèles d'inférence. Ces processus d'intelligence artificielle peuvent se dérouler en continu ou par lots à des moments précis (par exemple, une fois par jour, par semaine, etc.). Cette opération est généralement effectuée en nuage, car les systèmes périphériques ne disposent généralement pas de la puissance de traitement nécessaire. Pour plus d'informations, voir la section sur l'intelligence artificielle ci-dessous.
- La **communication de données à des chaînes de blocs** (dispositifs d'enregistrement électronique partagé) est utilisée dans l'exécution automatique des contrats intelligents (sujet qui sera abordé plus loin dans la section sur la technologie de la chaîne de blocs).

V. Gestion et sécurité de l'IoT

46. La sécurité des écosystèmes d'objets connectés doit protéger les données contre les attaques externes qui pourraient compromettre ou détruire l'écosystème et protéger en outre la confidentialité et l'intégrité des données. Certains des risques les plus importants pour les écosystèmes d'objets connectés sont les suivants :

- Les attaques de type « homme du milieu », au cours desquelles des pirates informatiques interceptent et volent ou modifient des données lors de leur transmission sur des réseaux ouverts ;
- Les attaques par des réseaux zombies, lors desquelles un pirate prend le contrôle d'un certain nombre de dispositifs en exploitant les failles de sécurité de ces dispositifs afin d'utiliser leurs ressources informatiques ;
- Les rançongiciels ou autres logiciels malveillants qui, s'ils sont installés sur des dispositifs IoT, peuvent mettre en péril l'ensemble d'un écosystème d'objets connectés.

47. Un cadre de cybersécurité permettant de faire face à ces menaces doit inclure un processus de dénomination et d'enregistrement des dispositifs bien défini, un système solide d'authentification des dispositifs, des protocoles permettant aux dispositifs de communiquer en toute sécurité au sein du réseau, ainsi qu'une plateforme de gestion des dispositifs tout au long de leur cycle de vie, y compris la possibilité de désactiver ou d'isoler un dispositif s'il devient « déviant ». Le principe de conception fondé sur la confiance zéro, qui ne permet aux composants d'une architecture d'objets connectés de communiquer que lorsqu'ils ont été spécifiquement autorisés à le faire, est un cadre sûr qui limite considérablement la capacité des composants de perturber d'autres services s'ils sont contaminés.

48. La gestion des dispositifs est un défi majeur, tant du point de vue de la sécurité que de l'exploitation. Contrairement aux systèmes informatiques classiques, les systèmes IoT comportent de nombreux dispositifs qui peuvent être dispersés en divers endroits et se trouver dans des environnements qui les rendent vulnérables, que ce soit matériellement ou au niveau de leurs connexions au réseau. En outre, les systèmes d'objets connectés doivent être faciles à reconfigurer en raison de l'évolution des technologies et des applications. Pour ces raisons, il est recommandé de toujours connaître le niveau d'avancement de chaque dispositif IoT et du logiciel qu'il contient et de disposer de mécanismes fiables pour donner des instructions à distance, notamment pour modifier les paramètres et mettre à jour le logiciel.

A. Fonctionnement et mise à jour des dispositifs

49. Pour pouvoir mettre à jour et reconfigurer facilement les systèmes IoT, il est essentiel de disposer d'un mécanisme fiable de mise à jour du logiciel des dispositifs connectés. Pour réduire le coût des mises à jour, les logiciels doivent être divisés en modules, dont les paramètres et les réglages peuvent être mis à jour à distance. La possibilité de modifier uniquement les paramètres, ou uniquement les modules pris séparément, permet de réduire au minimum les mises à jour et d'en augmenter le niveau de détail, ce qui réduit les coûts de télécommunications et autres. La mise à jour à distance des dispositifs est appelée micrologiciel « over-the-air » (OTA)[23].

50. Les deux solutions technologiques suivantes sont importantes pour la gestion et la mise à jour des dispositifs :

- Un **agent de messagerie**[24] (comme le protocole MQTT décrit plus haut) agit en quelque sorte comme un tiers de confiance pour renforcer la sécurité, car il ne reçoit que les messages des « éditeurs » autorisés. Ensuite, les dispositifs IoT « souscrivent un abonnement » auprès de l'agent et demandent périodiquement les informations pour lesquelles ils se sont abonnés (c'est-à-dire que la distribution fonctionne à la demande, et non selon l'offre). Pour les mises à jour logicielles, l'agent de messagerie peut, au lieu d'envoyer la totalité de la mise à jour, envoyer une adresse à laquelle le dispositif IoT peut se rendre pour télécharger la mise à jour. Les agents de messagerie simplifient la gestion, notamment grâce à l'utilisation de communications asynchrones, de sorte que si un dispositif IoT est temporairement hors service ou occupé, il recevra tout de même le message ou la mise à jour lorsqu'il sera de nouveau en ligne ou en mesure de se mettre à jour, l'agent de messagerie gardant quant à lui la trace des abonnés qui auront reçu le message et de ceux qui ne l'auront pas reçu. Il n'est pas nécessaire par ailleurs d'établir une liste centrale de tous les dispositifs à mettre à jour, car ces dispositifs sont enregistrés en tant qu'abonnés auprès de l'agent de messagerie au moment de l'installation ;
- Les logiciels et les mises à jour des dispositifs IoT peuvent être conçus pour appliquer l'**idempotence**[25]. Cela signifie que lorsqu'une action est répétée, le résultat est toujours le même que lorsqu'elle a été exécutée pour la première fois. Par exemple, si la même mise à jour logicielle ou la même modification de paramètres est accidentellement effectuée deux fois (ou même 100 fois) sur le même dispositif IoT, le résultat sera toujours le même.

51. De nombreux éléments des architectures d'objets connectés reposent sur des composants logiciels libres, ce qui signifie qu'il est souvent rapide de remédier aux failles de sécurité. Cependant, durant la période entre la découverte de la faille et la correction, le dispositif est vulnérable. Les systèmes et la vitesse de mise à jour des dispositifs IoT sont donc particulièrement importants.

52. Lors de la conception des systèmes de gestion des écosystèmes d'objets connectés, il est également important de garder à l'esprit les impératifs suivants :

- La conception et la mise à jour doivent s'appuyer sur des modèles empiriques de gestion des incidents touchant les écosystèmes d'objets connectés. Il n'existe pas encore de normes de gestion des incidents de ce type, mais on peut être sûr que de tels incidents se produiront, car le fonctionnement en situation réelle n'est jamais parfait. Il n'existe pas non plus de normes de gestion des incidents touchant les dispositifs IoT lorsque ceux-ci sont utilisés avec la technologie de la chaîne de blocs, ni d'indications sur la manière dont les modèles actuels de gestion des incidents pourraient être appliqués à ces

[23] Pour de plus amples renseignements, voir https://predictabledesigns.com/how-to-update-embedded-firmware-over-the-air-ota.

[24] Pour plus d'informations sur les agents de messagerie, voir https://www.ibm.com/cloud/learn/message-brokers#.

[25] Pour une explication de l'idempotence, voir https://medium.com/@ahmadfarag/idempotency-764f7bb6e4e2.

technologies. Il n'existe que des normes génériques applicables au partage des informations, telles que les normes ISO/CEI 27010, 20614, 20247 et 19592[26].

- Les aspects juridiques doivent être pris en compte lors de la conception des activités de collecte, de conservation, d'analyse, de suppression et de partage des données.

Contrôle de l'état des dispositifs

53. Outre un mécanisme permettant de mettre à jour le logiciel (micrologiciel) d'un dispositif IoT, un mécanisme est nécessaire pour connaître précisément l'état du dispositif. Cela signifie, au minimum, un registre indiquant la configuration logicielle actuelle ainsi que les configurations logicielles antérieures, un registre des opérations logicielles et un relevé des communications du dispositif.

B. Sécurité et vérification des dispositifs

54. Parce que les données générées par l'IoT peuvent être utilisées pour prendre des décisions (par exemple, verser ou non une indemnisation) ou pour élaborer des modèles d'inférence ou des contrats intelligents sur les réseaux de chaînes de blocs, il est nécessaire de s'assurer que les données sont véridiques et proviennent du monde réel.

55. Les solutions techniques permettant d'apporter cette garantie sont entre autres les suivantes :

Sécurité du réseau

56. Lors de la communication entre un dispositif et un système, ou entre plusieurs dispositifs, la protection contre les failles du réseau est généralement assurée par la mise en place d'un pare-feu autour du réseau d'objets connectés (ce qui renforce la sécurité des communications qui franchissent le pare-feu) et par le cryptage des communications.

Identité du dispositif

57. Le récepteur des données provenant du dispositif IoT doit vérifier que l'expéditeur est le bon partenaire. Cela se fait généralement au moyen d'une cryptographie à clef publique-privée permettant de communiquer l'identité du dispositif. Pour rendre ce processus encore plus sûr, l'utilisation de mécanismes de chaîne de blocs pour l'émission de certificats à clef publique pourrait devenir courante à l'avenir.

Vérification du logiciel

58. Bien que l'usurpation d'identité puisse être évitée grâce à l'utilisation de l'identité du dispositif, il est toujours possible que des données non autorisées soient transférées en raison de la modification du logiciel du dispositif. Ce risque peut être évité par une vérification et un enregistrement continus de l'état du logiciel. Par exemple, le logiciel du dispositif peut périodiquement faire l'objet d'un hachage[27] et être enregistré dans une chaîne de blocs ou une autre base de données sécurisée où il ne peut pas être modifié (le logiciel n'est qu'un ensemble de chiffres, il est donc possible de le hacher comme s'il s'agissait d'un très grand nombre). Ensuite, chaque fois qu'il y a une modification de l'empreinte, celle-ci peut être comparée au registre du dispositif afin de voir si la nouvelle empreinte correspond au résultat attendu d'une mise à jour. Pour plus de sécurité, les vérifications logicielles peuvent être effectuées dans des environnements d'exécution sûrs qui utilisent à la fois le matériel et le logiciel nécessaires pour isoler un programme des interférences externes[28].

[26] ISO/CEI 27010 − Gestion de la sécurité de l'information des communications intersectorielles et interorganisationnelles ; ISO 20614 − Protocole d'échange de données pour l'interopérabilité et la préservation ; ISO 20247 − Identifiant de document de bibliothèque international ; ISO 19592 − Techniques de sécurité − Partage de secret.

[27] Pour une définition/description du hachage, voir https://techterms.com/definition/hash.

[28] Pour plus d'informations sur les environnements d'exécution sûrs, voir https://blog.quarkslab.com/introduction-to-trusted-execution-environment-arms-trustzone.html.

VI. Technologies complémentaires

A. Intelligence artificielle

59. L'intelligence artificielle devient un élément essentiel de nombreux systèmes d'objets connectés, car les propriétaires de données et de systèmes cherchent à utiliser et à interpréter de grands volumes de données générées par l'IoT. En outre, l'IA, lorsqu'elle est combinée aux données générées par l'IoT, peut présenter divers avantages sur le plan de la facilitation du commerce, notamment dans le domaine de l'analyse des risques. Par exemple, elle pourrait permettre aux affréteurs et aux compagnies d'assurance de déterminer quelles cargaisons présentent le plus grand risque d'être endommagées ou détériorées. Elle pourrait également faciliter l'analyse comparative des routes de navigation et des méthodes d'expédition, ce qui n'était pas toujours économiquement réalisable auparavant.

60. L'intelligence artificielle utilise des processus d'« apprentissage profond » pour traiter de très grands volumes de données (mégadonnées), qu'elle utilise ensuite pour établir des « règles » d'évaluation des nouvelles données. Ces règles sont appelées « modèle d'inférence », modèle qui peut être mis à jour à mesure que des données supplémentaires sont reçues et analysées au cours des processus d'apprentissage profond.

61. L'apprentissage profond est très intensif sur le plan du calcul et nécessite une puissance et des ressources informatiques importantes. L'application du modèle d'inférence est beaucoup moins exigeante en ressources.

62. Par conséquent, dans les systèmes d'objets connectés plus avancés qui utilisent l'IA, on peut observer une décentralisation des charges de travail. En d'autres termes, l'apprentissage profond a lieu en nuage ou sur une autre plateforme centralisée, puis les modèles d'inférence qui en résultent, établis par l'IA, sont déployés sur les périphériques reliés à l'IoT pour « prendre des décisions » (par exemple, pour identifier les produits défectueux). Ces dispositifs informatiques périphériques et leurs modèles issus de l'IA peuvent également effectuer une évaluation préliminaire des nouvelles données avant que celles-ci ne soient transmises pour servir à un « apprentissage profond » plus poussé, réduisant ainsi la charge du côté du traitement en nuage par l'IA[29].

63. Si les données collectées par l'IoT sont soumises à des règles de confidentialité, l'un des moyens d'assurer le respect de ces règles est d'utiliser l'apprentissage fédéré associé à l'IA, qui consiste en différentes techniques de préservation de la confidentialité des données par un traitement local et/ou un cryptage[30].

1. Quelques étapes de la préparation et de la sauvegarde des données en vue de leur utilisation par l'IA

64. La plupart des données acquises par l'IoT à des fins de contrôle, d'exploitation ou autres peuvent être considérées comme des mégadonnées chronologiques[31]. Par conséquent, ces données peuvent être utilisées pour l'IA et l'apprentissage automatique, même si ce n'était pas l'objectif initial de leur collecte. À mesure que le coût de l'IA diminuera, les entreprises y auront davantage recours, ce qui augmentera la valeur des ensembles de données existants et plus anciens. Par conséquent, même si aujourd'hui elle n'utilise pas l'IA pour analyser les données qu'elle tire de l'IoT, une entreprise peut envisager de stocker ces

[29] Pour un article sur la formation contre l'inférence, voir https://blogs.gartner.com/paul-debeasi/2019/02/14/training-versus-inference/.

[30] Pour plus d'information sur l'apprentissage fédéré, voir https://towardsdatascience.com/how-federated-learning-is-going-to-revolutionize-ai-6e0ab580420f ; sur l'inférence, voir https://www.steatite-embedded.co.uk/what-is-ai-inference-at-the-edge/ ; sur l'IA en général, voir https://simpliv.wordpress.com/2018/08/14/what-is-ai/?.

[31] Les données chronologiques sont collectées au fil du temps et chaque élément de donnée est horodaté, ce qui signifie que les événements, les séquences d'événements et les intervalles de temps réguliers ou irréguliers entre ces événements peuvent être tracés et analysés. Comme dans les études à long terme, la valeur des données augmente en fonction de la durée de leur collecte. Pour plus d'informations, voir https://www.influxdata.com/what-is-time-series-data/.

données sous des formats « adaptés à l'IA » en vue d'une éventuelle utilisation future. Pour ce faire, elle doit garder à l'esprit deux considérations :

65. La première a trait à la manière de collecter en permanence des données qui soient telles qu'on puisse les traiter à l'avenir. Voici deux solutions technologiques possibles pour stocker de grandes quantités de données en vue d'un usage futur :

- **Lacs de données**[32] : stockage de données qui consiste à accumuler les données brutes acquises par l'IoT ;
- **Magasins de données**[33] : stockage de données qui consiste à stocker les données extraites du lac de données et traitées à des fins ou sous des aspects spécifiques.

66. La deuxième considération a trait à la préparation des données pour le traitement par l'IA. Pour cela, deux technologies couramment utilisées sont **MapReduce** et le **traitement de flux** :

- **MapReduce**[34] est un modèle libre de traitement des mégadonnées qui prend en charge le calcul parallèle, c'est-à-dire le calcul relatif à un même « problème » entrepris simultanément sur un groupe d'ordinateurs afin d'accélérer le traitement et l'analyse. MapReduce est couramment utilisé pour créer les données structurées nécessaires à l'IA et pour enregistrer les résultats dans un magasin de données afin de les utiliser comme données d'apprentissage profond.
- Les **données en continu**[35] sont des données horodatées générées en continu. Le processus de génération de ces données, appelé **traitement de flux**, peut être réalisé par inférence par l'IA (pour sélectionner les données intéressantes) ou simplement par l'affichage d'une alerte si une valeur donnée dépasse un seuil.

B. Technologie de la chaîne de blocs

67. La technologie de la chaîne de blocs permet à des parties distinctes d'accorder un degré de confiance plus élevé à une transaction, car les entrées dans un registre électronique (base de données) ne sont pas facilement falsifiables (c'est-à-dire qu'une fois les données écrites, il est extrêmement difficile de les modifier, sachant que la véracité dépend de l'exactitude des données dès le départ). Cette « immuabilité » s'explique par une combinaison de facteurs, comme le décrit la CEE dans son livre blanc sur la chaîne de blocs dans la facilitation du commerce[36], qui donne des informations détaillées sur cette technologie.

68. 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.

69. Une caractéristique supplémentaire de nombreuses chaînes de blocs qui rend les combinaisons IoT/chaîne de blocs attrayantes en tant que solution de facilitation du commerce est la possibilité de mettre en pratique des « contrats intelligents ». Ces contrats sont des programmes qui s'exécutent automatiquement dès qu'un ensemble de conditions

[32] Forbes, *What is a Data Lake?*, https://www.forbes.com/sites/bernardmarr/2018/08/27/what-is-a-data-lake-a-super-simple-explanation-for-anyone/#7122bc1b76e0.

[33] Pour une définition du magasin de données, voir https://searchdatamanagement.techtarget.com/definition/data-mart (lien vérifié le 11 octobre 2020). Cette référence comporte également un intéressant tableau de comparaison entre un lac de données, un magasin de données, un entrepôt de données et une base de données relationnelle.

[34] Pour plus d'informations au sujet de MapReduce, voir https://medium.com/edureka/mapreduce-tutorial-3d9535ddbe7c.

[35] Pour une présentation du traitement de flux, voir https://medium.com/stream-processing/what-is-stream-processing-1eadfca11b97.

[36] CEFACT-ONU, *White Paper on Blockchain in Trade Facilitation* (ECE/TRADE/457), 2020, disponible à l'adresse suivante : https://www.unece.org/fileadmin/DAM/trade/Publications/ECE-TRADE-457E_WPBlockchainTF.pdf.

convenues sont remplies, ce qui garantit une mise en œuvre rapide avec une interaction humaine minimale (et donc, souvent, des coûts moindres). Par exemple, un dispositif IoT qui transmet des coordonnées GPS à une chaîne de blocs peut, dans le cadre d'un contrat intelligent, signaler l'arrivée d'une expédition. Cela, à son tour, peut déclencher un paiement automatique. Cette automatisation de la prise de décisions permet d'accélérer l'exécution tout en réduisant les interventions humaines et les risques d'erreur ou de fraude. En outre, l'utilisation de la technologie de la chaîne de blocs a l'avantage d'ouvrir une voie d'information transparente et vérifiable.

70. Pour tirer parti de la nature inviolable des registres partagés, il est nécessaire d'effectuer des entrées directes à partir des dispositifs IoT qui sont la source des données (ou de leurs points d'accès à l'IoT). Cela permet de protéger les données générées contre toute suspicion d'altération (par un système intermédiaire).

1. Avantages de la combinaison de l'IoT et de la technologie de la chaîne de blocs en ce qui concerne la facilitation du commerce

71. Le cœur de tout écosystème d'objets connectés est l'orchestration des flux de données, qui porte sur les interactions entre les données et l'acheminement de ces données à destination et en provenance des dispositifs IoT, y compris les systèmes périphériques et les passerelles, l'informatique en nuage, les bases de données/chaînes de blocs et les applications logicielles d'exploitation et/ou d'analyse (y compris les contrats intelligents enregistrés sur une chaîne de blocs).

72. Alors que les aspects techniques de cette orchestration ont été examinés ci-dessus, les sections qui suivent traitent des facteurs à prendre en compte pour évaluer les avantages du déploiement de la technologie de la chaîne de blocs dans un écosystème d'objets connectés, compte tenu des forces et des faiblesses de cette technologie, et concluent par quelques exemples de la manière dont l'IoT est déjà combiné à la chaîne de blocs pour assurer une meilleure facilitation du commerce.

73. Comme indiqué dans l'introduction, la facilitation du commerce est « la simplification, la normalisation et l'harmonisation des procédures et des flux d'informations y afférents, qui participent au mouvement des marchandises entre le vendeur et l'acheteur et au paiement de celles-ci »[37]. Les processus commerciaux sont caractérisés par un volume élevé d'activités et de transactions répétitives, effectuées par un grand nombre de parties prenantes, conditions d'école pour l'utilisation à la fois de l'IoT et de la technologie de la chaîne de blocs avec les avantages décrits ci-dessous pour la facilitation du commerce.

Simplification

74. L'IoT utilisé conjointement avec la technologie de la chaîne de blocs, et en particulier l'utilisation de contrats intelligents, peuvent simplifier les processus en supprimant les acteurs intermédiaires dont le but principal est d'assurer l'authenticité des données et/ou de demander qu'une mesure soit prise sur la base de ces données. Désormais, les données peuvent provenir de dispositifs IoT, les « demandes » de prise de mesures peuvent provenir d'un écosystème d'objets connectés et/ou d'un contrat intelligent adossé à une chaîne de blocs et l'authenticité peut être garantie par un enregistrement sur une chaîne de blocs.

Normalisation

75. Les chaînes de blocs peuvent accroître la confiance dans les données partagées (ou communes) provenant des écosystèmes d'objets connectés, grâce à leurs capacités d'action suivantes :

- Faciliter une compréhension commune entre les parties prenantes, comme entre les entreprises expéditrices et destinataires ou entre une banque de financement du commerce et un exportateur. Par exemple, les parties prenantes peuvent accéder aux mêmes données vérifiables et utiliser ces données pour décrire les objets/événements

[37] Extrait du Guide pratique relatif à la facilitation du commerce, disponible à l'adresse suivante : https://tfig.unece.org/FR/.

liés aux conteneurs si ces derniers sont équipés de dispositifs IoT ou d'étiquettes/de codes lisibles par l'IoT, comme les codes NFC, RFID ou QR[38]. Ces codes peuvent être lus par d'autres dispositifs IoT et les informations recueillies peuvent être stockées sur une chaîne de blocs pour être accessibles.

- Déterminer de manière fiable la date et l'origine de chaque entrée en provenance d'un écosystème d'objets connectés. Par exemple, une banque de financement du commerce pourrait connaître le moment exact où les marchandises sont arrivées dans l'entrepôt de l'importateur, ou un assureur pourrait déterminer avec précision le moment où les marchandises ont été endommagées (et qui en avait la possession à ce moment-là).
- Vérifier les données générées par l'IoT avec un haut niveau de confiance, le recours à la cryptologie rendant ces données résistantes aux cyberattaques.

Harmonisation

76. Lorsqu'elle est utilisée avec l'IoT, la technologie de la chaîne de blocs favorise l'harmonisation pour les raisons suivantes :

- Toutes les parties prenantes disposant de « droits de lecture » des données de la chaîne de blocs peuvent consulter les mêmes données générées par l'IoT, qui sont accessibles à tous au même moment, ce qui apporte de la clarté et accroît les possibilités de collaboration.
- Les mêmes informations fournies par l'IoT sont enregistrées sur tous les nœuds de la chaîne de blocs.
- De par leur haut niveau de fiabilité, les chaînes de blocs renforcent l'intégrité des données saisies à partir des dispositifs IoT. Une chaîne de blocs ne peut pas vérifier les données (bien que les contrats intelligents puissent jouer un rôle dans la vérification) ; cependant, elle élimine les risques associés au point de vérité unique (source unique de données) créé lorsque les données générées par l'IoT sont enregistrées dans une base de données.

2. Inconvénients des chaînes de blocs et de l'IoT

77. Les limites et les inconvénients de l'utilisation de la chaîne de blocs ont fait l'objet de nombreuses études. Les points qui suivent ont trait à l'utilisation de la technologie de la chaîne de blocs associée à l'IoT à des fins de facilitation du commerce :

- Il est nécessaire de disposer de données de qualité car le principe « à données douteuses, résultats douteux » reste vrai avec les chaînes de blocs, bien que ce problème puisse être partiellement atténué par l'utilisation de contrats intelligents adossés aux chaînes de blocs pour évaluer la qualité des données avant qu'elles ne soient enregistrées sur une chaîne de blocs.
- Les normes de sécurité ne sont pas suffisamment élaborées pour pouvoir s'appliquer à des configurations de plateforme qui permettent à plusieurs utilisateurs d'utiliser un logiciel en commun, chacun n'ayant accès qu'à ses propres données (multilocation).
- Les réglementations sur la confidentialité des données peuvent rendre nécessaire d'examiner si les données générées par les dispositifs IoT sont écrites sur une chaîne de blocs partagée avec plusieurs parties prenantes.
- L'interopérabilité entre les chaînes de blocs n'est pas toujours facile à établir. Lorsqu'il existe plus d'une solution fondée sur la chaîne de blocs (par exemple, une

[38] La communication en champ proche (NFC) permet une communication à courte portée entre des dispositifs compatibles. L'identification par radiofréquence (RFID) utilise des champs électromagnétiques pour reconnaître et suivre automatiquement les étiquettes fixées aux objets. Un code à réponse rapide (QR) est un type de code-barres matriciel qui, dans ce cas, relie le lecteur à un localisateur URL spécifique.

solution utilisée par un transporteur et une autre par les douanes), si ces deux systèmes ne peuvent pas « communiquer », les informations peuvent rester cloisonnées.

78. L'IoT a été un atout pour la facilitation du commerce, car il a permis de rassembler des volumes jusque-là inégalés de données détaillées sur le commerce, dépassant de loin les systèmes antérieurs de collecte manuelle de données. Néanmoins, des lacunes subsistent dans les données et lorsqu'il y a des écarts, des distorsions ou des inexactitudes, ces défauts restent présents dans les données enregistrées sur une chaîne de blocs.

79. En outre, à moins que leurs mécanismes de gouvernance ou les contrats intelligents qui leur sont adossés n'en décident autrement, les chaînes de blocs sont des capteurs de données, enregistrant toutes les données commerciales qu'elles reçoivent sans aucun processus de sélection analytique. Cela pourrait poser un problème si toutes les données provenant d'un écosystème d'objets connectés étaient enregistrées sur une chaîne de blocs, car le volume de données généré pourrait entraîner à lui seul des défaillances du système et/ou des augmentations de coûts sur les réseaux qui perçoivent une petite redevance chaque fois que des données sont enregistrées sur une chaîne de blocs.

80. C'est la raison pour laquelle, bien que les dispositifs IoT puissent être un moyen utile de recueillir des données, généralement, toutes les données générées par l'IoT ne sont pas enregistrées sur une chaîne de blocs. Les données provenant des dispositifs IoT sont souvent filtrées de la façon suivante :

- Seules les données qui sortent des plages définies sont communiquées, ou
- Les données sont communiquées sous la forme d'un ensemble total de relevés à la fin d'un processus, ou encore
- Un « hash »[39] d'un grand volume de données recueillies sur une période définie avec précision est sauvegardé sur la chaîne de blocs, tandis que les données elles-mêmes sont sauvegardées ailleurs. Cette dernière option est intéressante car si on veut vérifier les données, on leur applique les fonctions mathématiques de hachage et si le résultat est différent de celui enregistré sur la chaîne de blocs, la partie qui effectue le contrôle sait que les données initiales ont été modifiées.

3. Deux exemples d'utilisation de l'IoT associé à la technologie de la chaîne de blocs pour faciliter le commerce

Mesure de la température à des fins d'assurance

81. Les fruits sont sensibles à la température et il est préférable de les conserver entre 4 et 15 degrés Celsius pendant le transport. Si, par exemple, pendant le transport, un dispositif IoT installé dans un conteneur de fret indique que les fruits ont été conservés à 0 °C pendant deux jours entiers, cela peut avoir des conséquences au niveau de l'assurance. En d'autres termes, lorsque le dispositif connecté transmet des températures hors plage, cette information, enregistrée sur la chaîne de blocs, peut activer un contrat intelligent, qui notifie à la compagnie d'assurance qu'un paiement doit être effectué à l'exportateur pour compenser la perte de marchandises due à une température trop basse. Ce paiement sera automatiquement effectué par le contrat intelligent sans aucune intervention de l'importateur, de l'exportateur ou de la société de transport. Cela réduit considérablement le coût du traitement des demandes d'indemnisation pour les compagnies d'assurance, celles-ci n'ayant pas à comparer les informations soumises par l'expéditeur/exportateur avec la police d'assurance, à évaluer la sincérité de la demande d'indemnisation (les données générées par l'IoT enregistrées sur une chaîne de blocs en fournissant la preuve), puis à demander le paiement. En outre, cela réduit les coûts pour l'expéditeur/exportateur, car celui-ci n'a pas à

[39] Un « hash » est une sorte d'empreinte cryptographique qui change si un seul caractère des données hashées change. Cela signifie que si un gigaoctet de données, ou même un chiffre ou un espace dans ces données, est modifié, le hash de tout le gigaoctet de données changera. Ce processus ne peut toutefois pas être utilisé pour déterminer à quel endroit la modification a été effectuée.

fournir d'autres documents sur le problème survenu et recevra plus rapidement l'indemnité versée par l'assurance[40].

Financement du commerce

82. Le système traditionnel de financement du commerce prévoit, pour l'obtention d'un financement, le transfert d'un connaissement au propriétaire de la cargaison, soit physiquement, soit par courrier électronique, et la comparaison des données du connaissement avec les récépissés d'entrepôt de la cargaison (les unes comme les autres pouvant faire l'objet d'une falsification). Une forme courante de fraude consiste à émettre plusieurs récépissés d'entrepôt pour les mêmes marchandises, puis à utiliser ces récépissés frauduleux pour obtenir un financement. L'IoT peut combattre la fraude en surveillant, en temps réel, les marchandises en transit et en entrepôt. Les données collectées par les dispositifs connectés et enregistrées sur une chaîne de blocs (pour prouver leur authenticité) peuvent ensuite être tracées par les parties prenantes ayant un accès en « lecture seule ». En outre, comme dans l'exemple précédent, lorsque les conditions sont remplies (par exemple, la cargaison est arrivée à temps), des contrats intelligents peuvent être activés pour mettre en œuvre des contrats de financement du commerce. En fournissant aux parties prenantes une source de données sûre et immuable, la combinaison des technologies de l'IoT et de la chaîne de blocs n'élimine pas la fraude, mais la rend plus difficile à commettre.

VII. Conclusion

83. Les transactions économiques impliquant des échanges transfrontaliers dépendent de l'accès à des données fiables et transmises en temps voulu. Les dispositifs IoT qui enregistrent les données sur une chaîne de blocs peuvent apporter une solution, en permettant aux utilisateurs d'accéder en temps réel aux informations, qu'il s'agisse des vendeurs, des acheteurs ou d'intermédiaires tels que les prestataires de services logistiques ou les agents des douanes. Les contrats intelligents − une caractéristique de la technologie de la chaîne de blocs − peuvent servir de mécanisme de recoupement automatique, facilitant l'exécution rapide des paiements lorsqu'un ensemble donné de conditions sont remplies. En outre, les chaînes de blocs sont relativement résistantes aux cyberattaques du fait qu'elles utilisent la cryptographie. Bien que les problèmes de qualité des données et d'interopérabilité soient communs à l'IoT et à la technologie de la chaîne de blocs, l'utilisation de cette combinaison peut être un instrument très efficace de facilitation du commerce.

[40] Cet exemple, accompagné d'une analyse plus complète, figure dans CEFACT-ONU, *White Paper on Blockchain in Trade Facilitation* (ECE/TRADE/457), 2020, disponible à l'adresse suivante : https://www.unece.org/fileadmin/DAM/trade/Publications/ECE-TRADE-457E_WPBlockchainTF.pdf.