Un nouvel outil numérique pour la fiabilisation des *supply chains* : *la blockchain*

Par Matthieu HUG
Serial entrepreneur, cofondateur et CEO de Tilkal

Les registres numériques distribués *(blockchains*) promettent de réinventer la confiance en rendant possibles des systèmes de notariat désintermédiés et décentralisés. Leur application à l'industrie financière, largement étudiée et commentée, pourrait modifier nos systèmes d'échanges basés sur des tiers de confiance.
D'autres applications de ces technologies visent, quant à elles, non pas simplement à se substituer aux mécanismes de confiance existants, mais bien à établir de la confiance là où celle-ci fait défaut. Une application ayant un intérêt sanitaire majeur est l'assurance de la traçabilité des produits de bout en bout, depuis le fabricant jusqu'au consommateur : d'abord pour fournir au consommateur la transparence qu'il réclame sur ce qu'il consomme, et la conformité, dont il veut pouvoir juger, par rapport à ses critères de santé ou d'éthique. Ensuite pour lutter contre l'incroyable croissance de toutes les formes de contrefaçon, qui touchent toutes les industries, du médicament aux aliments pour nourrissons, en passant par les pièces automobiles.

Depuis quelques années, les différentes formes de commerce illicite (contrefaçon et « marchés gris ») sont devenues la première manifestation de criminalité mondiale, avec un « chiffre d'affaires » de l'ordre de 1 000 milliards de dollars (qui les place bien avant le trafic de drogue). Ce que l'on croit cantonné au luxe dans l'imaginaire collectif européen concerne en réalité toutes les industries : du médicament aux pièces détachées automobiles, du lait pour enfants aux sachets de parmesan, des téléphones portables aux batteries, des jouets au vin et aux huîtres. Concrètement, à eux seuls, les médicaments contrefaits tuent 700 000 personnes dans le monde chaque année (par comparaison, le SIDA a fait 1,1 million de victimes en 2015). Ainsi, la traçabilité des produits et des biens est devenue un enjeu global de santé et de sécurité publique.

Si le risque reste pour l'instant relativement maîtrisé en Europe occidentale, ce fléau est devenu dramatique ailleurs dans le monde : l'organisme algérien de protection des marques déposées (Inapi) estime que 80 % des produits en vente dans ce pays sont des faux. Selon le laboratoire pharmaceutique Lilly, ce sont plus de 90 % des médicaments vendus en ligne qui relèveraient du commerce illicite. Et cette situation s'aggrave rapidement : globalement, les contrefaçons et les marchés illicites ont connu une croissance d'un facteur 10 au cours des 10 dernières années. Plusieurs éléments expliquent cette situation :

- l'essor du e-commerce (en particulier, des places de marché) a facilité l'écoulement des produits détournés ou falsifiés, générant une forte demande d'approvisionnement en amont ;
- cet appel d'air sur la distribution en ligne a favorisé la structuration d'une véritable chaîne d'approvisionnement illicite à l'échelle globale, couvrant les matières premières, la fabrication, la vente en gros, les transports ou la logistique ;
- ces *supply chains* illicites sont massivement interconnectées aux *supply chains* légitimes, échangeant, mélangeant, substituant des produits à tous les niveaux et à toutes les étapes ;
- l'ampleur du trafic illicite : avec 1 000 milliards d'euros en jeu, ceux qui s'y livrent ont globalement plus de moyens financiers pour l'organiser qu'aucun industriel seul n'en a pour les contrer. Ainsi, lorsqu'en 2013, 28 laboratoires pharmaceutiques mondiaux lancent le financement sur 3 ans d'un programme de lutte avec Interpol, il s'agit de 5,9 millions de dollars, résultant de la saisie de faux médicaments pour 81 millions de dollars en 2015 (à comparer à un marché global du faux médicament de probablement 150 à 200 milliards de dollars…).

En bout de chaîne, l'exigence grandissante de transparence de la part des consommateurs est donc largement justifiée.

Établir la continuité de l'information

Face à l'utilisation du numérique pour globaliser la distribution de produits issus des chaînes illicites, les approches de fiabilisation des chaînes industrielles légitimes ont, à l'évidence, été déficientes. Certes, les dispositifs de marquage physique des produits et des biens se sont développés et même multipliés. Mais alors que les *supply chains* se sont globalisées, les informations issues de ces dispositifs de marquage restent confinées à chaque intervenant : en clair, il n'existe dans pratiquement aucune industrie de connaissance consolidée et fiable du cycle de vie réel d'un produit, qu'il s'agisse de sa localisation à un instant T, de ses conditions de transport, de son lieu de vente ou de son éventuel reconditionnement (*repackaging*).

Cette rupture de la chaîne des informations nous rend aveugles : elle permet les trafics illicites. En la palliant, on peut espérer réaliser deux avancées importantes :

- la création d'une identité numérique du produit constituée de son cycle de vie consolidé. Étant indépendante et de nature différente du marquage physique, cette identité numérique crée les conditions d'une véritable authentification forte des produits ;
- une analyse statistique, grâce à des algorithmes spécialisés, de l'ensemble des cycles de vie permettant de détecter les anomalies, que ce soient des indicateurs de trafics illicites ou des sources d'amélioration du fonctionnement de la chaîne d'approvisionnement.

À partir d'une identification unique opposée sur le produit, les actions effectuées sur celui-ci sont déclarées à chaque étape de sa *supply chain*, depuis sa production jusqu'à son utilisation finale (par exemple, sa provenance, son origine, ses conditions de fabrication ou de stockage, sa mise sur palette, son transport en conteneur, etc.). En bout de chaîne, l'identité numérique ainsi constituée peut être lue par un consommateur (avec un *smartphone*) en s'appuyant sur le marquage unique du produit (par exemple, un QR code). Cette lecture en bout de chaîne est en soi un événement de la *supply chain* qui est lui aussi constitutif de l'identité numérique du produit : on voit que l'on a là, d'ores et déjà, un mécanisme simple et unitaire qui permet de détecter en temps réel des produits inconnus, des reconditionnements anormaux, voire des ventes dans des zones géographiques non autorisées.

La mise en œuvre d'une telle plateforme pose des questions techniques évidentes, mais pas insolubles, de volumétrie d'information et de performance d'accès. Au-delà, elle pose surtout des questions complexes de confiance, au sens large du terme. Tout d'abord, chaque intervenant doit partager des informations relatives à son activité : cela pose une question évidente non seulement de confidentialité, mais aussi de transparence. Ensuite, il y a un risque grave d'effet « pot de miel » : une information centralisée serait inévitablement la cible de cyberattaques et de piratages, compte tenu des enjeux. Il faut donc consolider sans centraliser, et partager tout en garantissant la confidentialité. Enfin, il y a la question de la fiabilité des données.

Pourquoi la *blockchain* ?

Les questions de confidentialité et de consolidation décentralisée amènent naturellement à l'idée d'un registre numérique décentralisé (*blockchain*). Mais cette technologie peut-elle être utilisée à bon escient dans le cadre des *supply chains* et, si oui, comment ?

D'un point de vue fonctionnel, la technologie *blockchain* peut être vue comme une base de données distribuée qui enregistre des transactions séquentiellement dans le temps et interdit leur modification ultérieure : régulièrement, un groupe de transactions est créé, ce bloc référence explicitement le précédent, puis il est soumis à validation, par consensus de tout ou partie des participants au registre. Une fois validé, un bloc devient vite très difficile à modifier, et il en va de même pour toutes les transactions qu'il contient : il faudrait pour cela modifier en même temps tous les blocs ultérieurs et tromper le mécanisme de consensus appliqué par tous les autres participants. D'un point de vue technique, on peut aussi voir la technologie *blockchain* comme un protocole de synchronisation de données opérant directement sur la couche logicielle de plus bas niveau dans un réseau, offrant ainsi une surface d'attaque plus faible que des protocoles de plus haut niveau.

À partir de ces deux points de vue, de nombreuses variations (parfois interdépendantes) sont possibles : mécanismes de consensus, participation ouverte au consensus ou limitée à des membres pré-identifiés, accès public ou privé aux données échangées, celles-ci étant chiffrées ou non, etc. Les configurations choisies varient naturellement en fonction du problème que l'on cherche à résoudre. Dans tous les cas, on voit que la *blockchain* est un composant technologique qui rend un service précis, à savoir l'établissement d'une confiance consensuelle. Celle-ci repose sur deux piliers : sa non-répudiabilité (la donnée peut servir de « preuve ») et son inaltérabilité en tous cas à un coût « raisonnable ». La question cruciale est alors de savoir autour de quelle information, précisément, l'on veut (et l'on peut) établir ce consensus de confiance.

La mise en œuvre

Dans le cas des *supply chains*, on va utiliser un registre numérique distribué et privé à deux fins : organiser un réseau de collecte d'informations et prouver ultérieurement, grâce à celles-ci, l'origine et le contenu de chaque élément constituant l'identité numérique du produit. Ce registre est partagé entre des nœuds qui sont tous connus et identifiés individuellement : ce sont les intervenants de la *supply chain* concernée, typiquement les fournisseurs, les industriels, les transporteurs, les distributeurs, voire les institutionnels. Il va donc s'agir d'une *blockchain* dite « à permission » pour laquelle on peut appliquer un algorithme de consensus plus simple que dans le cas des *blockchains* publiques (et donc bénéficier de performances bien meilleures qu'avec ces dernières).

La collecte des informations auprès de chaque intervenant de la *supply chain* se fait localement, au sein de son

système d'information, *via* un nœud packagé avec une couche d'API (interface de programmation applicative) : l'information est ensuite recopiée par le protocole sur chaque nœud du réseau. Les nœuds du réseau appartenant *a priori* à différents acteurs industriels, chaque information est chiffrée avec une clé propre à chaque nœud afin d'assurer la confidentialité.

On utilise ainsi la *blockchain* pour créer la confiance sur deux dimensions : l'origine de l'information et son inaltérabilité (son intégrité dans le temps). La confidentialité de l'information est gérée par des mécanismes de chiffrement avancés en amont de la *blockchain*. La scalabilité de l'accès aux données ainsi que leur consolidation et leur agrégation statistique sont, quant à elles, gérées en aval sur des données extraites de la *blockchain*, mais qui référencent celle-ci. À aucun moment ne se pose la question de la véracité des informations entrées dans le registre par les intervenants : une information fausse reste une information qu'il est fondamental de capturer. C'est l'analyse de la *supply chain* à partir des informations fournies par les intervenants, que celles-ci soient vraies ou fausses, qui permettra de détecter les « faux » et de les corriger. De fait, l'objectif n'est pas de constituer un registre d'informations « vraies » : cela n'aurait aucun sens, car cela présupposerait que toutes les malveillances et toutes les erreurs auraient été résolues, et donc que le problème initial des *supply chains* décrit plus haut l'aurait été également. L'objectif est de constituer un registre d'informations qui ne soient pas modifiables afin d'être en mesure, en les analysant, de détecter des problèmes et d'établir une boucle de rétroaction transparente, laquelle, progressivement, fiabilisera l'ensemble de la *supply chain* en responsabilisant chacun des intervenants.

Ce mécanisme est notablement évolutif : il n'est pas nécessaire que tous les intervenants de la *supply chain* fournissent de l'information, puisque même une vue partielle permettra d'amorcer la boucle de rétroaction. En outre, un nouvel intervenant qui se connecte au système n'a qu'à déployer son nœud : une fois celui-ci autorisé dans le réseau, le protocole *blockchain* assurera sa synchronisation avec le reste du réseau. Chaque nouvel intervenant connecté au réseau augmente à la fois la sécurité du réseau, la transparence globale et la pertinence de la rétroaction. La *blockchain* est donc un mécanisme propre à unir progressivement des acteurs industriels ayant à la fois des intérêts et des valeurs en commun.

D'autres points sont à traiter pour un déploiement industriel de la *blockchain*, notamment l'archivage des données ou encore le cadre juridique (en particulier en ce qui concerne les données personnelles). Des réponses existent, mais dépassent le cadre de cet article. Au-delà des tests initiaux, la question désormais posée est celle de l'utilisation de cette brique technologique, en conjonction avec d'autres, pour résoudre des problèmes se posant à une échelle industrielle.

Conclusion

Les technologies de registre numérique distribué, ou *blockchain*, apportent une brique de confiance. L'approche envisagée ici n'est pas de chercher à utiliser une technologie pour forcer la confiance entre les participants à la *blockchain*, ni même pour avoir confiance dans les données qu'ils déclarent dans la *blockchain* : cela reviendrait à résoudre à l'avance le problème posé. Dans ce contexte, on crée les conditions pour que les informations ne soient pas altérées : l'intégrité des données, leur quasi immutabilité, est au cœur de la confiance garantie par le registre numérique distribué. Grâce à cette immutabilité, on peut utiliser des algorithmes d'analyse des cycles de vie des produits tels que déclarés par les intervenants d'une *supply chain* et y détecter des signaux faibles caractéristiques d'anomalies, quelle qu'en soit la nature (dysfonctionnement, malveillance, irrégularité, non-qualité, etc.). On génère ainsi une boucle de rétroaction permettant de responsabiliser chaque intervenant et, *in fine,* de fiabiliser le fonctionnement des *supply chains*. C'est une logique d'amélioration continue similaire à une approche de type *lean manufacturing* qui est ainsi mise en place, mais à l'échelle d'une filière industrielle. Cette amélioration continue établit les conditions de la transparence, base d'un nouveau contrat de confiance avec le consommateur.

Références bibliographiques (en ligne)

Eli Lilly & Co, *Integrated Report 2015*, Part Operating Responsibly.

http://fightthefakes.org

International Chamber of Commerce.

OCDE, *Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact*, 2016.

Europe & UN-OHIM, *2015 Situation Report on Counterfeiting in the European Union*, April 2015.

2016, KPMG and AGMA, *Gray Markets Report.*

ONUDC, *Le Trafic illicite de biens contrefaits et la criminalité transnationale organisée*, 2014 : http://www.unodc.org/documents/counterfeit/FocusSheet/Counterfeit_focussheet_FR_HIRES.pdf