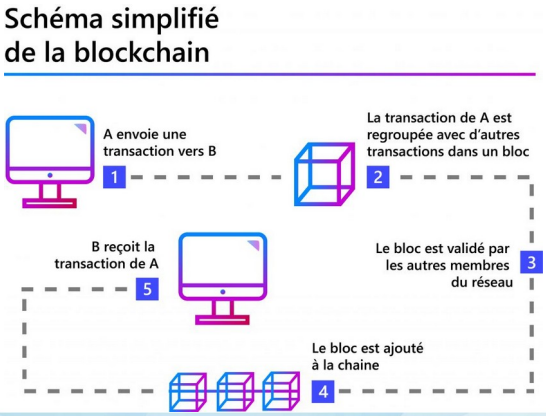
LES NOTES DU CREOGN

Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale

Numéro 70 – Mars 2022

Mathéo GILBERT



LA TECHNOLOGIE BLOCKCHAIN DANS L'INDUSTRIE DE LA LOGISTIQUE

Les difficultés au sein des chaînes logistiques sont, d'abord, celles de la multiplication des intermédiaires qui résultent, notamment, de l'allongement des distances à couvrir pour répondre aux besoins d'approvisionnement. Cela crée une croissance des éléments administratifs et du nombre de personnes concernées par l'activité. À cela s'ajoute la difficulté d'authentification des informations, des acteurs et des produits[1]. On peut aussi noter les problématiques de traçabilité des matériaux lors de leur construction et de leur acheminement[2]. Chacune de ces problématiques peut être résolue par la technologie blockchain, qu'il s'agisse de l'industrie agroalimentaire, de l'industrie aéronautique ou de celle de l'armement. Des entreprises l'utilisent d'ores et déjà[3]. La blockchain permet la mise en place d'un processus de vérification et d'authentification des informations, ainsi qu'une traçabilité des éléments. De plus, la transparence d'une blockchain permet d'identifier la perte, le vol ou la fraude et, ainsi, de mieux sécuriser les matériaux.

I) La blockchain, système informatique de sécurisation et de transmission de la donnée

a) Qu'est-ce que la blockchain, et comment fonctionne-t-elle ?

La blockchain est une technologie informatique. La première est née en 2009 avec celle du Bitcoin. Elle est utilisée de nos jours par toutes les cryptomonnaies. Blockchain signifie « chaîne de blocs ». C'est un registre informatique où des données peuvent être ajoutées pour ne plus être modifiées ni effacées. La blockchain, dans son essence, assure la sécurité des informations qui y transitent. Elle est aussi un garant d'authentification. C'est un registre puisqu'elle enregistre et horodate chacune des données circulantes. Les informations sont incrémentées manuellement ou automatiquement (par numérisation de documents, par sondes, par outils de mesure…)[4]. La blockchain fonctionne sur un système de consensus qui permet de garantir la synchronisation entre tous les nœuds du réseau et l'authenticité de chaque donnée. Il existe plusieurs mécanismes de consensus : la preuve de travail, la preuve d'enjeu, la preuve d'enjeu déléguée ou encore la preuve d'importance[5]. Quant à la sécurité des informations circulant dans le réseau, elle est garantie par le système de hachage. Ce dernier transforme un input (une donnée qui peut être un texte) en une suite fixe d'éléments alphanumériques, l'output. L'output, aussi appelé « digest », est la valeur de hachage. Le hachage sert à identifier une

1 CHANUT, Guillaume. Blockchain et chaîne logistique – Un bon cas d'utilisation ? *Cryptoast*, 20 octobre 2019. Disponible sur : https://cryptoast.fr/blockchain-supply-chain/

2 Utiliser la blockchain dans sa chaîne logistique. *AGROMedia.fr*, 9 avril 2020. Disponible sur : https://www.agro-media.fr/dossier/utiliser-la-blockchain-dans-sa-chaine-logistique-41211.html

3 Nestlé et Carrefour inaugurent la première blockchain en nutrition infantile. *nestle.fr,* 21 novembre 2019. Disponible sur :https://www.nestle.fr/media/pressreleases/blockchain-guigoz

4 « Blockchain Applications for Industry 4.0 and Industrial IoT : A. Review. *IEEE Xplore Access*. Disponible sur : https://ieeexplore.ieee.org/abstract/document/8917991

5 Les principaux protocoles de consensus. *Journal du coin*. Disponible sur : https://journalducoin.com/lexique/blockchain-consensus-pow-pos-dpos/

donnée. Il ne peut faire transparaître la moindre information, tant sur l'input que sur l'output. Ainsi, pour un input donné, il ne peut y avoir qu'un seul output.[6] Le système de hachage crée un jumeau numérique qui est l'empreinte numérique de la donnée initiale. La traçabilité fonctionne grâce au hachage. Chaque opération de transfert requiert un hash qui crée un digest. La blockchain est composée de blocs qui regroupent les hash effectués. Chaque bloc crée un nouveau hash, lequel sera le premier hash du bloc suivant. Ainsi, la moindre modification est identifiable, puisqu'elle modifie l'intégralité de la blockchain, ce qui rend visible pour tous toute tentative de fraude. La numérisation des informations, la fiabilité des échanges et transactions ainsi que la transparence du registre à l'égard de ceux qui sont autorisés à l'accès, permettent de réduire drastiquement des pertes de temps et d'énergie humaine et matérielle, sans besoin d'un tiers de confiance. Ainsi, par exemple, un individu qui crée un compte utilisateur sur une plateforme web déposera un mot de passe et un identifiant. Le fournisseur de la plateforme n'aura pas connaissance du mot de passe. Il l'exécutera et le convertira avec le système de hachage pour créer un « condensat » (aussi appelé « digest » ou « output »). Par conséquent, lors d'une reconnexion, l'utilisateur va rentrer ses identifiants et le fournisseur vérifiera la concordance entre les éléments rentrés et le condensat. S'il y a conformité, alors l'accès est ouvert. Le hachage est à différencier du chiffrement qui, lui, transforme une donnée en une forme inintelligible par quiconque n'ayant pas connaissance de la clé de chiffrement. Par conséquent, du fait de la numérisation généralisée de l'information, la blockchain peut répondre aux enjeux de sécurité, tout en simplifiant le processus d'acheminement et de traitement de l'information. À cela s'ajoutent les « smart contracts », aussi appelés « contrats intelligents », qui permettent, grâce à des conditions définies par l'informatique, d'automatiser le processus contractuel.

b) Blockchain et contrats intelligents en chaîne de logistique

La technologie blockchain permet d'assurer à chaque partie participant à l'acheminement d'un matériau ou d'un produit la connaissance exacte du cycle de création. Ainsi, s'il y a nécessité de vérifier le trajet d'un produit ou encore les personnes qui participent à l'assemblage, ainsi que tout autre élément nécessaire à l'enquête en cas de litige, il suffit d'étudier les blocs de la chaîne qui ont authentifié et horodaté chaque personne participante et chaque étape. Ce sont des informations sécurisées et authentifiées par le système de hachage. Un autre élément qui fait la force de la blockchain, est la logique pair-à-pair (P2P) qui définit la sécurité de la blockchain et des données qui y circulent. Les données sont hébergées par l'ensemble des ordinateurs connectés au réseau. Il n'est donc pas nécessaire d'avoir une entité qui gouverne la gestion des données, contrôle les activités et assure la sécurisation de la blockchain. Celle-ci s'administre seule et automatiquement. La blockchain, si elle est décentralisée, s'affranchit donc des tiers de confiance. Ainsi, si l'on y ajoute les contrats intelligents, chaque activité est réglementée et définie au préalable et la gestion des données circulantes est assurée. Si la blockchain est suffisamment complexe et dotée d'une capacité de calcul élevée, il est possible de doter celle-ci des contrats intelligents. Ils permettent, grâce à des conditions établies au préalable, de déclencher par exemple des transferts d'actifs lorsque les conditions sont remplies. Ils sont régis par le droit commun des contrats (Code civil) et ne se différencient pas des contrats d'usage. La blockchain, additionnée à l'utilisation des contrats intelligents, permet de redéfinir les fonctionnements des chaînes logistiques ainsi que de résoudre les enjeux et les difficultés des chaînes logistiques, puisqu'ils permettent d'assurer le respect de la conformité et l'efficacité des processus. En effet, les contrats intelligents permettent d'automatiser la totalité du processus. Mais ils ne font pas qu'automatiser, ils restreignent et réduisent les actions intermédiaires, augmentant ainsi la productivité et limitant la production de documentation. De plus, ils effacent les risques d'erreurs et de fraudes, notamment dans les accords contractuels. La blockchain garantit l'absence de défauts ou de modification des contrats. Efficacité, sécurité et transparence sont les mots d'ordre de la blockchain.[7]

c) Blockchain publique ou privée ?

Les blockchains publiques sont aux blockchains privées ce que l'Internet est aux Intranets. Un Intranet est créé pour une entité. Par ailleurs, une blockchain privée a comme avantage sa rapidité. Le réseau étant fermé et peu complexe (car moins de nœuds) du fait de la faible quantité d'utilisateurs, le consensus requis est plus rapide à obtenir et les phénomènes de congestion sont peu probables. Cependant, la blockchain privée présente comme désavantages l'insécurité du réseau et sa centralisation (on parle donc aussi de blockchain centralisée). L'insécurité se justifie par la nécessité de devoir faire confiance aux utilisateurs qui doivent valider eux-mêmes les nœuds du réseau, c'est-à-dire l'information transmise. Les acteurs externes à l'activité et au protocole devront donc faire confiance à l'utilisateur en charge de la vérification de la donnée, sans aucune possibilité de contrôle. De plus, moins de complexité du réseau, et donc moins de nœuds, signifie une plus grande facilité pour le réseau d'être corrompu et manipulé. Quant à la centralisation, elle présente la problématique d'avoir un système central de gestion des données. Ainsi, en cas d'incident de cybersécurité sur ce système

6 Qu'est-ce que le hachage dans une transaction blockchain ? Disponible sur : https://www.bitpanda.com/academy/fr/lecons/quest-ce-que-le-hachage-dans-une-transaction-blockchain/

7 La blockchain en logistique : rapidité et sécurité de l'entrepôt. *mecalux.fr,* 22 avril 2021. Disponible sur : https://www.mecalux.fr/blog/blockchain-logistique

central, les données peuvent être endommagées et/ou volées. Quant à la blockchain publique, elle ne rend pas nécessairement toutes ses transactions publiques. Elle est considérée comme telle car le réseau est accessible à tous. Elle peut ne faire transparaître que les hash. Ainsi, seuls les tiers de confiance et les utilisateurs eux-mêmes peuvent reconnaître la donnée transmise. Les échanges effectués sur son réseau peuvent être vus uniquement au travers d'une adresse, aussi appelée clé de signature. En effet, les données proviennent d'une clé pour parvenir à une autre. Et seuls ceux qui ont connaissance de la personne derrière la clé sont en mesure d'en identifier l'origine. Aussi est-il impossible informatiquement d'empêcher une transaction. L'intégralité du système de la blockchain est créé en ce sens, pour sécuriser et assurer un parfait traitement de l'information transférée ou déposée.

d) Les véritables avantages d'une blockchain publique

Une entreprise qui évolue dans le secteur de la logistique et des transports, dotée d'une blockchain, dispose de quatre grands avantages. Le premier est le gain de temps, du fait des transactions qui peuvent s'effectuer en temps quasi réel. Le deuxième est la grande réduction des coûts, puisqu'il n'y a pas nécessité d'avoir recours à un tiers de confiance pour évaluer les coûts ni gérer les litiges. Il s'agit aussi de supprimer les tâches redondantes pour optimiser la productivité générale. Ensuite, la mise en place d'une blockchain signifie une numérisation quasi totale de l'entreprise. Cela a un coût, mais c'est avant tout un véritable investissement au regard de l'ensemble des bénéfices que cette technologie offre. En effet, au-delà des aspects d'optimisation des processus, la blockchain, lorsqu'elle est publique, est une véritable solution de sécurité et de gestion des identités. Elle protège contre la falsification et la fraude. L'organisation qui se dote d'une blockchain remodèle son modèle économique. À ces bénéficies s'ajoute la sécurité des données, dont l'accès peut être échelonné sur plusieurs niveaux selon les services et les degrés de confidentialité.

e) La blockchain comme outil de simplification des processus internes

La blockchain réunit la donnée immatérielle. Un document, une fois numérisé, devient immatériel. C'est la création du jumeau numérique. En tant que registre, la blockchain facilite les processus administratifs. Elle permet de corroborer les données relatives à l'écosystème financier, et simplifie, par exemple, le travail du comptable. De plus, les stratégies managériales et financières sont construites à la suite de la simple interprétation des données du réseau, qui donnent lieu à des synthèses utiles pour l'amélioration logistique des processus. En sa qualité de registre accessible à plusieurs acteurs, la lecture voire l'écriture de la donnée est ouverte à d'autres organisations. Ainsi, les administrations judiciaires et fiscales, par exemple, peuvent avoir accès aux données de l'entreprise. Cela permet de simplifier les processus judiciaires pour la récolte d'informations relatives à une enquête. L'administration fiscale peut avoir un droit de lecture sur les informations comptables pour vérifier les informations transmises lors de la déclaration faite aux services des impôts des entreprises (SIE). La blockchain est donc, en plus d'être un registre, un système permettant la collaboration d'acteurs. Quant à l'authenticité des données traitées grâce à l' « effet de réseau », elle permet de rendre légitimes les intervenants quant à leurs compétences. Chacun, grâce à la vérification des utilisateurs, devient digne de confiance. Cela permet d'effacer les moindres doutes relatifs à un défaut de compétence d'un acteur de la chaîne logistique. La traçabilité, quant à elle, assouplit grandement les soucis de qualité ou de défaut d'acheminement, puisqu'elle permet de posséder une correspondance fiable et permanente entre l'actif physique et son jumeau numérique.[8]

II) Les utilisations futures de la blockchain

a) L'utilisation des contrats intelligents dans l'industrie

Dans l'industrie de la logistique et du transport, il sera décidé, comme condition, que l'arrivée d'un matériau soit enregistrée puis authentifiée dans la blockchain. Une fois effectuée et terminée, chaque étape de l'acheminement verrouille la validation d'une condition. Dans cet exemple, cela déclenche le transfert d'un actif financier et sa division auprès de chacun des acteurs ayant participé à l'acheminement du produit. Un autre usage des contrats intelligents pourra être notamment celui des assurances. En cas de défaillances relatives à une livraison (annulation, retard, matériel abîmé) par exemple, le contrat intelligent déclenchera une condition précise qui permettra au client de percevoir un avoir, un actif financier ou toute autre compensation. Ainsi, un contrat auto-exécutant étant créé sur une blockchain, il est non modifiable, incorruptible et est donc protégé de toute fraude ou non-respect des normes contractuelles établies.

8 DE COËTLOGON, Perrine, DURAND, Marc, JEANTET, Maxime, GÉNIN, Claire, RAMON, Romuald, et al.. Les technologies blockchain au service du secteur public. [Rapport de recherche] Université de Lille (2018-..). 2021. hal-03232816v. Disponible sur : https://hal.archives-ouvertes.fr/hal-03232816/document

b) La mutualisation de la technologie blockchain et des objets connectés

Les objets connectés sont des objets qui enregistrent leur propre cycle de vie. Ainsi, en cas d'application d'une technologie blockchain en chaîne de logistique, si l'on y ajoute l'utilisation des objets connectés, ceux-ci peuvent tout à fait incrémenter continuellement les informations qui leurs sont relatives, directement dans le réseau. Cela nécessitera un travail ultérieur de traitement de ces données qui auront été rassemblées et catégorisées dans le réseau. Par ailleurs, l'utilisation des objets connectés permet de piloter la chaîne logistique en temps réel. L'utilisation des balises RFID (Radio Frequency IDentification), la radio-identification, est destinée à mémoriser et récupérer des données (température, état du matériel, vitesse) à distance grâce à des marqueurs, appelés « radio-étiquettes ». Cela permet d'optimiser l'efficience du processus de prise de décision. En logistique, cela offre aussi une meilleure gestion des flux physiques des produits. Ainsi, les problématiques relatives à la fraude, aux défauts, aux contaminations alimentaires ou encore au vol, pourront être évitées ou identifiées rapidement, pour donner lieu à des diagnostics rapides. La totale transparence des informations circulant sur le réseau, avec une parfaite traçabilité des informations, permet une grande capacité de résilience.

c) Sécurisation de l'information sur blockchain par chiffrement asymétrique

La réception et la transmission des informations sont des enjeux majeurs au sein des armées. De ce fait, l'utilisation d'une blockchain publique pourrait être très intéressante. En effet, on peut imaginer qu'un gendarme puisse valider une opération *via* une blockchain. Pour cela, il utilisera sa signature électronique pour valider l'opération, qui générera un hash unique qui sera incorporé dans la blockchain. Un exemple pourrait être l'arrivage d'un convoi d'armes militaires de la gendarmerie. Une fois la réception effectuée, l'agent en charge de celle-ci répertorie le bon arrivage dans la blockchain sous forme de texte, lequel est modifié par le protocole de hachage pour devenir un « digest » unique (1 hash = 1 digest), dont la traduction pourra être faite seulement par une clé publique détenue par le chef de service. Ainsi, l'usage d'une blockchain publique permettra d'intégrer l'information au travers de millions d'autres, avec une totale impossibilité pour qui que ce soit d'identifier la donnée transmise. Car, bien que l'utilisateur puisse être identifié grâce à son identité numérique (uniquement auprès de son supérieur dans l'exemple précédent), l'anonymat est complet. C'est un chiffrement asymétrique qui est utilisé, ce qui nécessite une clé publique pour chiffrer et une clé privée pour déchiffrer.

III) Les obstacles à l'implémentation de la technologie blockchain

Cette technologie apporte de nombreux avantages, offre de nombreuses possibilités, et s'inscrit dans un contexte de besoins auxquels elle peut répondre. Cependant, la plus grosse problématique est la possibilité que les acteurs qui incrémentent la donnée soient malintentionnés. En effet, dans ces applications, la blockchain va nécessiter l'appui d'Oracles. Ils sont les sources d'informations qui permettent d'intégrer des variables issues du monde réel dans des contrats intelligents. Or, si les données incrémentées par l'Oracle dans le réseau sont fausses, corrompues ou inexactes, le réseau va tout de même les authentifier comme justes et les incrémenter dans les autres blocs du réseau. L'ensemble des autres acteurs ne pourra que se fier à l'authentification du réseau sans avoir la possibilité de déterminer la mauvaise foi de l'acteur initial de la donnée. Dans l'industrie de la logistique et du transport et, *a fortiori*, dans l'industrie de l'armement ou agroalimentaire, si l'on veut établir une technologie blockchain pour bénéficier de ses avantages, il est fortement nécessaire d'élaborer des règles strictes à suivre lors de l'incrémentation, ainsi que de prévoir un contrôle et une surveillance du processus. Il serait aussi utile de former et de sensibiliser sur les risques et peines encourus en cas de détection de fausses données implémentées. Ces recommandations, même appliquées, ne garantissent cependant aucunement la bonne foi des utilisateurs et ne rendent pas possible la détection de la mauvaise donnée dans le réseau. C'est d'ailleurs la raison pour laquelle seul le transfert de cryptoactifs est aujourd'hui fonctionnel, puisqu'il crée la donnée pour que celle-ci soit ensuite transférée de pair-à-pair, sans nécessiter d'interactions avec le monde réel.

Mathéo GILBERT *est apprenti en master 1 Intelligence économique au CREOGN.*