ceis

Septembre 2018

Blockchain

Enjeux, usages et contraintes pour la Défense

Par Axel Dyèvre et Suzanne Mc Namara

Les notes stratégiques

L'intelligence de la décision

Les notes stratégiques

Notes d'étude et d'analyse

Les idées et les opinions exprimées dans ce document n'engagent que les auteurs et ne reflètent pas nécessairement la position de CEIS ou des experts rencontrés.

CEIS est une société d'études et de conseil en stratégie. Sa vocation est d'assister ses clients dans leur développement en France et à l'international et de contribuer à la protection de leurs intérêts. Pour cela, les 80 consultants de CEIS associent systématiquement vision prospective et approche opérationnelle, maîtrise des informations utiles à la décision et accompagnement dans l'action.

CEIS met en œuvre et anime le DGA Lab, le laboratoire d'innovation du ministère de la Défense www.defense.gouv.fr/dga/innovation2/dga-lab

La Direction Générale pour l'Armement a initié en 2013 un centre de réflexion sur l'innovation et un espace de démonstrations de technologies innovantes dans le domaine des systèmes d'informations, le SIA Lab (**www.sia-lab.fr**), créé et animé par CEIS sous la responsabilité du Groupe Sopra Steria, Architecte-intégrateur du programme SIA.

Forte du succès de cette initiative, la DGA a étendu en 2016 le périmètre de ce centre à l'ensemble des domaines technologiques d'intérêt pour la Défense et a lancé le DGA Lab. Espace de démonstration technologique mais aussi de réflexion collaborative sur les usages des nouvelles technologies, le DGA Lab est ouvert à l'ensemble des acteurs de l'innovation de défense, au premier rang desquels les opérationnels du ministère de la Défense.

Le DGA Lab est mis en œuvre et animé par la DGA avec le concours des sociétés CEIS et Sopra Steria.

Dans ce cadre de cette activité, les consultants de CEIS publient des Notes Stratégiques portant notamment sur les questions relatives aux impacts de la transformation numérique pour la Défense.

Travaillant étroitement avec les équipes de CEIS et le DGA Lab, le **Bureau Européen de CEIS** à Bruxelles, conseille et assiste les acteurs publics, européens ou nationaux, ainsi que les acteurs privés dans l'élaboration de leur stratégie européenne, notamment sur les problématiques de défense, sécurité, transport, énergie et affaires maritimes. CEIS - Bureau Européen participe également à des projets de recherche européens dans ces domaines. Pour mener à bien l'ensemble de ses missions, l'équipe s'appuie sur un réseau européen de contacts, d'experts et de partenaires.

Contact :

Axel Dyèvre

adyevre@ceis.eu

CEIS

Tour Montparnasse

33 avenue du Maine

75755 Paris Cedex 15

+33 1 45 55 00 20

CEIS - Bureau Européen

Boulevard Charlemagne, 42

B-1000 Bruxelles

+32 2 646 70 43

DGA Lab

40, rue d'Oradour-sur-Glâne

F-75015 Paris

+33 1 84 17 82 77

www.ceis.eu

Retrouvez toutes les Notes Stratégiques sur **www.ceis.eu** et **www.sia-lab.fr**

Sommaire

Synthèse

La blockchain (« chaîne de blocs ») est une technologie qui fait beaucoup parler d'elle depuis quelques années.

Il s'agit d'un système de gestion distribuée de bases de données : les acteurs membres d'une blockchain ont - pour simplifier - tous une copie à jour de la base de données complète, mais ils ne peuvent pas modifier les entrées existantes (appelées « blocs ») et les nouvelles entrées doivent être validées pour être ajoutées à cette « chaine ».

Les « blocs » contiennent donc les données et sont reliés entre eux par des liens cryptographiques. Le concept de sécurité et de traçabilité des blockchains repose sur le fait que lorsqu'une transaction a été faite, elle est validée, horodatée et ajoutée à la chaîne. Ensuite, un bloc et les données qu'il contient ne peuvent théoriquement plus être modifiés sans que cela ne soit détecté.

Il existe trois types de blockchain, dont les conditions de fonctionnement varient, ce qui a un impact notamment sur les modes de validation des opérations et donc sur la sécurité des données :

- Les **blockchains publiques** (comme la cryptomonnaie Bitcoin) sont ouvertes à tout individu via Internet. Elles ne présentent pas de barrière à l'entrée. La validation des transactions repose sur la notion de consensus décentralisé, puisqu'elle s'affranchit d'une autorité centrale de contrôle.
- La **blockchain hybride** est une blockchain dont la gouvernance est partiellement décentralisée entre plusieurs entités qui forment un consortium. Celui-ci peut, par exemple, être constitué d'institutions financières ou d'entreprises. L'accès en est donc limité et la validation

des transactions fonctionne souvent avec des règles de type « vote majoritaire » : au moins la moitié des acteurs doivent valider les transactions.

- Les **blockchains privées** sont, elles, soumises à des barrières à l'entrée et à une gouvernance centralisée. Pour rejoindre la blockchain, les participants doivent être acceptés par l'entité qui l'administre. C'est cette entité centrale qui définit les règles de fonctionnement (droits d'écriture et de lecture) de la chaîne. C'est sans doute la blockchain privée qui correspondrait le mieux aux usages possibles pour la Défense.

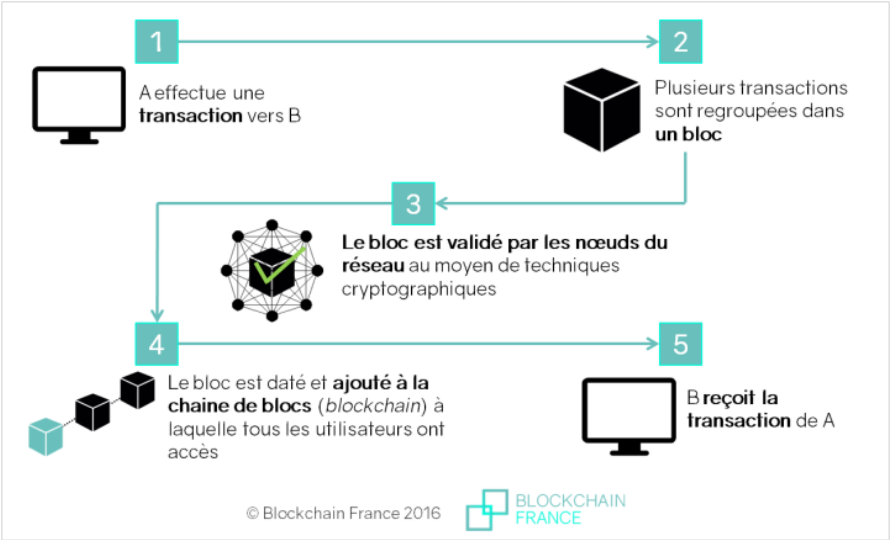
En dépit de quelques limites, la blockchain semble présenter des caractéristiques indéniablement intéressantes pour la Défense française. Sa résilience, sa disponibilité et son inviolabilité en font un atout significatif pour différentes applications : messagerie sécurisée, gestion des identités et des fichiers RH, suivi logistique. C'est la notion de sécurité et d'immuabilité qui la rend particulièrement pertinente pour le domaine militaire. La blockchain pourrait en effet offrir au secteur de la Défense un stockage des données ultra-sécurisé et consultable à tout instant par les individus accrédités.

Largement expérimentée dans le civil, la blockchain a d'abord été promue et utilisée par les start-ups et elle convainc maintenant peu à peu les grandes entreprises. Les États (USA, Russie, etc.) et les organisations internationales (ONU, OTAN, Union européenne, etc.) commencent à s'y intéresser également. L'ampleur du phénomène est réelle, même s'il n'existe pas, à ce jour, d'usages véritablement déployés à grande échelle en dehors des cryptomonnaies.

Cependant, comme pour toute nouvelle technologie a priori prometteuse, certains alertent sur le manque de visibilité quant à la résilience à long terme de la blockchain. Elle doit bien évidemment être expérimentée et soigneusement évaluée avant d'être introduite dans le milieu de la Défense française.

Fonctionnement et usages de la technologie blockchain

La blockchain est avant tout un système de gestion distribuée de bases de données. Il s'agit d'une chaîne de « blocs », liés entre eux par des liens cryptographiques. Les blocs contiennent de la donnée. Pour être ajouté à la chaîne, un nouveau bloc doit être validé par les participants à la chaîne. Il est ensuite horodaté et devient immuable : les données qu'il contient ne peuvent plus être modifiées, sauf si l'ensemble des participants à la chaîne (ou ceux autorisés, s'il s'agit d'une blockchain privée) valident la modification. Une blockchain est donc un historique des transactions qui se veut infalsifiable.



Le fonctionnement de la blockchain, par Blockchain France

Typologie des blockchains

Il existe trois types de blockchains : publiques, privées et hybrides[1].

Blockchains publiques (blockchains unpermissioned)

Les blockchains publiques sont ouvertes à tout individu via Internet. Elles ne présentent pas de barrière à l'entrée. N'importe qui peut les consulter ou les utiliser, c'est-à-dire se constituer en nœud de réseau et participer à la validation des transactions et au chaînage des blocs. Le fonctionnement d'une blockchain publique repose sur la notion de consensus décentralisé, puisqu'elle s'affranchit d'une autorité centrale de contrôle : ce sont les noeuds qui assurent le fonctionnement de la chaîne et la validation des transactions. Les blockchains publiques les plus connues sont celles du Bitcoin et d'Ethereum.

Blockchains privées (blockchains permissioned)

Les blockchains privées, qui correspondent le mieux à un usage défense, sont soumises à des barrières à l'entrée et à une gouvernance centralisée. Pour rejoindre la blockchain, les participants doivent être acceptés par l'entité qui l'administre. C'est cette entité centrale qui définit les règles de fonctionnement (droits d'écriture et de lecture) de la chaîne. Elle peut décider de valider les transactions et d'ajouter les blocs à la chaîne elle-même, ou bien elle peut désigner un ou plusieurs nœuds qui seront autorisés à la faire. Une blockchain privée ne repose donc pas sur le principe même du consensus décentralisé : les règles de son fonctionnement sont établies à l'avance par l'entité créatrice et le consensus est contrôlé par un ou plusieurs nœuds « dirigeants ». Ce type de blockchain est particulièrement adapté à un usage en entreprise, puisqu'il permet notamment de faciliter le travail

[1] « Blockchain : état des lieux et perspectives », janvier 2018, CEIS ; https://solutions.lesechos.fr/tech/c/part-v-blockchain-privee-publique-difference-9229/

collaboratif[2]. Une blockchain privée offre une maîtrise de la confidentialité et des accès qui est impossible dans le cadre d'une blockchain publique. Une des blockchains privées les plus connues est l'Hyperledger Fabric[3], une plateforme open source de développement de chaîne de blocs, utilisée notamment par IBM. Développée depuis fin 2015 par la fondation Linux, Hypeledger « *regroupe différents frameworks permettant de développer des contrats intelligents ou des applications décentralisées dans la blockchain, à destination des entreprises* ».

Blockchains hybrides, ou « de consortium »

Une blockchain hybride est une blockchain dont la gouvernance est partiellement décentralisée entre plusieurs entités : le consortium. Le consortium peut par exemple être constitué d'institutions financières ou d'entreprises. La blockchain hybride est privée dans son fonctionnement mais, contrairement à une blockchain privée, la gouvernance est partagée entre plusieurs entités, c'est-à-dire que le consensus est contrôlé par un ensemble prédéterminé de nœuds. Dans une blockchain publique, les participants sont anonymes et il n'y a pas de régulateur centralisé. Dans le cas du fonctionnement d'une banque ou d'une entreprise par exemple, l'identité des participants est cependant nécessaire. Ainsi, comme pour une blockchain privée, l'accès à la chaîne hybride est filtré et peut être modifié. Ce sont les membres du consortium, c'est-à-dire les entités gouvernantes de la blockchain qui définissent le consensus : ils définissent notamment combien de nœuds doivent valider les transactions pour que celles-ci soient ajoutées à la chaîne (il s'agit le plus souvent de la majorité). Le droit de lecture d'une blockchain de consortium est également déterminé par les entités gouvernantes : il peut être public ou limité aux participants de la chaîne.

[2] « Blockchain : état des lieux et perspectives », janvier 2018, CEIS ; https://solutions.lesechos.fr/tech/c/part-v-blockchain-privee-publique-difference-9229
[3] https://www.hyperledger.org/projects/fabric

Corda, créée en 2016 par le consortium de banques « R3 », est une blockchain hybride composée d'organisations du secteur financier.

Modes de validation des transactions

Les modes de validation des transactions sont les règles qui régissent le fonctionnement de la blockchain.[4]

Dans le cas des blockchains publiques, le fonctionnement de la chaîne est assuré par les « mineurs » : il s'agit des personnes (en fait de leurs machines) jouant le rôle de « nœuds de réseaux ». Elles se chargent des calculs nécessaires à la vérification et à la validation des transactions et de l'ajout des blocs à la blockchain. La validation se fait essentiellement de deux façons :

- par une « **preuve de travail** » (*proof of work*, aussi appelée « preuve de calcul »), un procédé cryptographique qui consiste à résoudre un problème mathématique complexe et nécessitant donc une certaine puissance de calcul informatique. Le premier mineur à résoudre le problème est autorisé à créer le prochain bloc et à l'ajouter à la chaîne.
- par une « **preuve de détention** » (*proof of stake*, aussi appelé « preuve d'enjeu »), qui ne nécessite pas l'utilisation de la puissance de calcul pour résoudre un problème complexe, mais qui demande aux mineurs de prouver la propriété -selon la blockchain considérée- d'un certain montant de cryptomonnaie ou d'un certain nombre d'actifs. La sélection du mineur est donc pondérée par la quantité de cryptomonnaie ou d'actifs qu'il possède.

[4] « Blockchain : état des lieux et perspectives », janvier 2018, CEIS ; https://solutions.lesechos.fr/tech/c/part-v-blockchain-privee-publique-difference-9229

Il existe néanmoins une trentaine d'autres méthodes de validation des transactions, moins connues et usitées, parmi lesquelles[5] :

- La « **preuve d'importance** » (*proof of importance*) : le mineur est sélectionné selon des critères tels que son utilisation de la blockchain, son ancienneté et la quantité de cryptomonnaie/d'actifs qu'il possède.
- La « **preuve d'activité** » (*proof of activity*) : la sélection du mineur dépend de son activité, ce qui agit comme une incitation à utiliser la blockchain.
- La « **preuve de capacité** » (*proof of capacity*) : le mineur est sélectionné selon sa capacité de stockage.
- La « **preuve de possession** » (*proof of hold*) : plus l'utilisateur conserve ses actifs dans la durée, plus il aura de chance d'être sélectionné pour valider le bloc.
- La « **preuve d'autorité** » (*proof of authority*) : cette règle concerne les blockchains **privées** et de consortium. La preuve d'autorité est l'autorisation d'un ou plusieurs nœuds à ajouter des blocs. La blockchain, bien que restant distribuée, perd ainsi son caractère décentralisé.

Apports et bénéfices

La blockchain se caractérise par sa résilience, sa traçabilité, son intégrité et sa disponibilité.

Résilience

De par sa structure distribuée, la blockchain est un système très résilient, qui permet une meilleure résistance aux attaques. De plus, les blocs frauduleux sont

[5] https://www.senat.fr/fileadmin/Fichiers/Images/opecst/quatre_pages/OPECST_2018_0020_note_blockchain.pdf ; https://cryptoast.fr/qu-est-ce-que-pos-proof-of-stake/ ; https://www.cryptoencyclopedie.com/single-post/Quest-ce-que-le-consensus-Proof-of-Work-

automatiquement identifiés : chaque nœud vérifie la validité du bloc et les blocs erronés se retrouvent donc rapidement mis à l'écart.

Traçabilité

La traçabilité est rendue possible par l'horodatage de chaque transaction et l'inviolabilité des blocs. Cela permet de pouvoir retrouver facilement l'intégralité de l'historique de la chaîne. Sa traçabilité fait de la blockchain une technologie particulièrement intéressante pour, par exemple, le suivi de la chaîne logistique.

Intégrité

L'intégrité de la blockchain réside dans le fait que les blocs ne peuvent pas être modifiés. La modification d'un bloc contenu dans une chaîne publique ne peut se faire qu'à l'unanimité des participants, ce qui est très peu probable dans le cas d'une chaîne de grande ampleur. Les données contenues dans les blocs sont donc théoriquement infalsifiables.

Accenture travaille actuellement sur le développement d'une blockchain privée modifiable. Cela permettra à l'administrateur central d'une chaîne privée de modifier ou de supprimer certains blocs sans pour autant briser la chaîne. La modification des blocs est rendue possible par l'utilisation d'une forme de « hachage caméléon » : l'administrateur possède des clés de sécurité privées lui permettant d'éditer les blocs et de recréer les algorithmes les liant entre eux.[6]

Cette innovation n'est en revanche pas destinée aux blockchains publiques. Permettre à tous les participants d'une blockchain publique de la modifier serait en effet très risqué en termes de sécurité des données. La blockchain perdrait de fait son intégrité. L'immutabilité d'une blockchain publique peut toutefois avoir des effets pervers : si des informations préjudiciables sont

[6] https://newsroom.accenture.com/news/accenture-debuts-prototype-of-editable-blockchain-for-enterprise-and-permissioned-systems.htm

présentes sur une chaîne publique, un individu malveillant pourrait s'en servir à mauvais escient sans qu'il soit possible de les supprimer de la blockchain.

Disponibilité

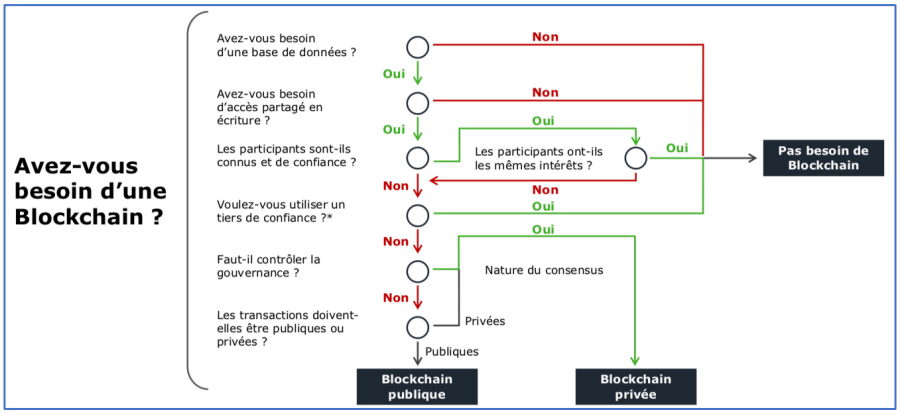
La disponibilité et la résilience du système sont garanties puisque l'historique des transactions est consultable à partir de chaque nœud du réseau. Si certains nœuds sont défaillants ou disparaissent, l'historique reste consultable sur les autres nœuds. La disponibilité est donc le corollaire du caractère distribué de la blockchain.

La blockchain présente également l'avantage de proposer une structure de coûts alternative, souvent plus avantageuse qu'un système centralisé : les coûts de développement, de gestion et de transactions seraient plus faibles que ceux générés par le recours à une autorité centrale. A titre d'exemple, la digitalisation de la validation des transactions pour des domaines comme le transport logistique permet une réduction importante des coûts de fonctionnement. Un système de blockchain en entreprise peut également, grâce au consensus, fluidifier les échanges et favoriser le travail collaboratif et donc la productivité en général.

Application possibles de la blockchain pour la Défense

Les usages possibles de la technologie blockchain dans la Défense reposent sur l'utilisation de **blockchains privées**, dont le fonctionnement et les accès seraient exclusivement déterminés et contrôlés par les services du ministère des Armées.

L'usage de blockchains publiques dans le cadre d'activités militaires, par définition sensibles, ne saurait être envisagé puisque l'accès aux chaînes ne serait pas contrôlé. L'usage de blockchains de consortium pourrait quant à lui être envisageable dans le cadre d'une gouvernance inter-services ou inter-unités.



Blockchain, Panorama des technologies existantes, Deloitte, 2017

Messageries sécurisées

En 2016, la DARPA[7] américaine a lancé un appel d'offres pour son projet « Secure Messaging Platform », un service de messagerie ultra-sécurisée dont l'objectif serait de transférer des messages via un protocole décentralisé[8]. Dans son article « La blockchain, nouvelle botte secrète des armées ? »[9], le cabinet SIA Partners explique que cette messagerie, dégagée de toute autorité centrale, fonctionnerait grâce à une clé de chiffrement qui ne rendrait les données échangées « *lisibles que par le destinataire final, mais la diffusion du message crypté à l'ensemble du réseau garanti[rait] la stabilité du système de messagerie et la confidentialité des métadonnées, l'émetteur et le récepteur devenant impossibles à identifier pour un tiers. Cela constitue[rait] un progrès par rapport au système actuel, dans lequel les données sont inégalement distribuées, les rendant vulnérables à une défaillance des serveurs, liée ou non à une démarche hostile* ». Un tel système permettrait donc d'échanger plus facilement, et de manière sécurisée.

Dans le civil, des applications de messageries instantanée basée sur la blockchain commencent à voir le jour. L'application Status, par exemple, fonctionne grâce à la blockchain Ethereum et se revendique ainsi « *privée, sécurisée et non censurable* »[10]. Grâce à la blockchain, basée sur une technologie *peer-to-peer*, l'avantage premier de ce type de messagerie est l'absence de serveurs entre les utilisateurs. Les échanges entre utilisateurs ne peuvent donc par être utilisés, par exemple, à des fins commerciales ou politiques. Une messagerie telle que Status est par conséquent très

[7] Defense Advanced Research Projects Agency : agence du Département de la Défense des États-Unis chargée de la recherche et développement des nouvelles technologies destinées à un usage militaire.
[8] http://www.defnat.com/pdf/Kempf%20(T%201011).pdf ; « Blockchain : état des lieux et perspectives », janvier 2018, CEIS
[9] http://secteur-public.sia-partners.com/20180301/la-blockchain-nouvelle-botte-secrete-des-armees
[10] https://mybroadband.co.za/news/software/268265-the-most-private-and-secure-messaging-platform-in-the-world-and-why-it-is-better-than-whatsapp.html

compliquée à bloquer ou à censurer, comme l'a fait la Russie avec Telegram, le Brésil et la Chine avec WhatsApp ou encore l'Iran avec Google. Si une telle utilisation de la blockchain peut représenter un risque, par exemple par l'usage de ce type de messageries sécurisées par des groupes terroristes, elle pourrait également présenter un intérêt pour les échanges internes aux Armées et, pourquoi pas, le partage rapide d'informations critiques en opération. Ce dernier usage se heurte toutefois à la problématique de l'accessibilité aux réseaux sur certains théâtres d'opération.

Gestion des identités numériques

La confidentialité des données personnelles semble aussi pouvoir être sécurisée par la technologie blockchain. Il deviendrait ainsi possible de créer une identité numérique infalsifiable puisque stockée dans une blockchain. Le programme alimentaire mondial de l'ONU a par exemple développé une plateforme de paiement basée sur la blockchain destinée à venir en aide aux réfugiés du camp d'Azraq, en Syrie, en leur permettant notamment d'acheter de la nourriture auprès de fournisseurs locaux[11]. En Birmanie, une ONG a lancé un projet pilote de distribution aux réfugiés Rohingya de cartes d'identité numériques utilisant la technologie blockchain, afin de favoriser leur accès à différents services[12]. Enfin, fin 2017 à New York, la start-up Blockchain for Change a mené un projet de distribution de smartphones à des personnes sans abris[13], afin que celles-ci créent leur identité digitale sur une blockchain et puissent ainsi accéder à divers services (accès aux foyers d'accueil, aux distributions de nourriture, etc.), recevoir de l'argent des

[11] https://www.crypto-france.com/blockchain-programme-alimentaire-mondial-onu-contournement-frais-bancaires/ ; ; https://coin24.fr/2018/02/21/programme-alimentaire-mondial-de-lonu-economise-milliers-de-dollars-grace-a-technologie-blockchain/
[12] https://www.challenges.fr/monde/une-carte-d-identite-blockchain-pour-les-rohingyas_555888
[13] https://lesclesdedemain.lemonde.fr/technologie/un-projet-blockchain-pour-donner-une-identite-digitale-aux-personnes-sans-domicile-fixe_a-88-6454.html

organismes gouvernementaux et effectuer des paiements grâce à une cryptomonnaie ad hoc, le « *change coin* ».

Dans un contexte Défense, il est facile et pertinent de considérer l'usage du stockage sécurisé des identités numériques des combattants. Un tel registre pourrait par exemple être utilisé pour homogénéiser, si ce n'est remplacer, des documents tels que les journaux de marche de l'armée de Terre, les carnets de vols de l'armée de l'Air et les journaux de bord de la Marine. Une blockchain offrirait un registre sécurisé distribué entre les différentes unités et consultable à tout moment par les participants à la chaîne. Elle permettrait également la validation (quasi) instantanée de la présence des combattants sur les théâtres d'opération.

Logistique et suivi du matériel sensible

La technologie blockchain est une réponse intéressante aux problématiques de traçabilité et de suivi logistique. Elle pourrait améliorer la traçabilité des transactions impliquant des biens ou des pièces détachées. Le partage d'une base de données entre les fournisseurs et le(s) destinataire(s) offrirait en effet une visibilité renforcée du parcours des produits. Cela permettrait une meilleure traçabilité des transactions effectuées tout au long de la chaîne logistique et une identification rapide des fraudes (une entité ne pourrait pas modifier ou supprimer unilatéralement des informations de la chaîne). Les domaines d'applications potentiels sont nombreux : l'agroalimentaire, pour un suivi plus fiable des opérations relatives aux produits alimentaires ; les transports internationaux, pour, entre autres, une diminution des frais de vérification des marchandises et des délais de transit ; l'industrie pour une meilleure traçabilité des transactions impliquant des pièces détachées ou des

produits tels que des médicaments ; le luxe, pour améliorer la traçabilité et lutter contre la contrefaçon ; etc.[14]

La mise en œuvre au sein du ministère des Armées de blockchains pour le suivi logistique des équipements en général et du matériel sensible en particulier permettrait une traçabilité sécurisée tout au long de leur cycle de vie. En juillet 2018, Accenture et Thales ont présenté un système basé sur la blockchain et permettant de sécuriser et de rationaliser les chaînes logistiques des secteurs de l'aéronautique et de la défense.[15] Ce système, encore au stade de prototype, est basé sur la blockchain Hyperledger Fabric et permet la traçabilité et l'authentification des pièces et matériaux utilisés sur les avions, ainsi qu'un enregistrement infalsifiable des transactions. Le registre, et donc la visibilité de la chaîne logistique, est partagé par tous les acteurs concernés : fournisseurs, fabricants et opérateurs. Les Armées pourraient sans doute tirer profit d'une solution analogue, qui leur permettrait de posséder un registre unique mais partagé de chaque transaction effectuée tout au long de leurs chaînes logistiques, notamment dans le cadre du suivi du matériel sensible (armes, substances toxiques, etc.). Chaque opération impliquant les pièces et les matériaux utilisés serait donc enregistrée et horodatée. En cas de problème ou de dysfonctionnement, cette traçabilité améliorée offrirait la possibilité de retrouver la pièce défectueuse et de connaître beaucoup plus rapidement et facilement le moment exact de son entrée dans la chaîne et son parcours tout au long de celle-ci. Enfin, le coût de vérification serait moindre puisque tout le processus serait dématérialisé.

De plus, de nombreuses entreprises civiles, parfois basées à l'étranger, prennent place dans les chaînes logistiques militaires. Il pourrait être intéressant de mettre en oeuvre une application logistique utilisant une blockchain dédiée et garantissant un système unifié et distribué de traçabilité

[14] https://www.airbus.com/newsroom/news/en/2017/03/Blockchain.html ; http://blockchainpartner.fr/supply-chain-tracabilite-blockchain/
[15] https://www.accenture.com/fr-fr/company-news-release-accenture-thales-demonstrate

et d'audit, que chaque entreprise pourrait alimenter et que le ministère pourrait consulter facilement. Ce système pourrait néanmoins se heurter à quelques limites, notamment la capacité de stockage de la chaîne.

Limites de la blockchain

Coût et consommation énergétique

Dans le cadre des blockchains publiques, les limites principales évoquées par les experts reposent sur le coût et la lenteur des transactions, ainsi que sur l'importance de la consommation énergétique. La validation et l'ajout des blocs à la chaîne du bitcoin, par exemple, se fait par « preuve de travail » : plusieurs milliers d'ordinateurs sont mis en concurrence pour résoudre un calcul très complexe afin de valider la transaction. Un seul ordinateur résoudra le calcul et sera rémunéré pour cela : les autres travaillent donc pour rien et sont à l'origine d'une importante déperdition d'énergie. Dans le cas du bitcoin, la blockchain a entrainé la création d'immenses « fermes » informatiques composées de centaines de milliers d'ordinateurs (cf. la « ferme » islandaise Enigma[16]).

Ce dispositif consomme annuellement une énergie supérieure à la consommation totale de certains pays : en août 2018, la consommation énergétique annuelle du bitcoin (environ 73 Térawatt par heure) se rapproche de celle d'un pays comme l'Autriche (72 TWh)[17]. De plus, contrairement aux promesses de la blockchain de réduire les temps de transactions grâce à l'affranchissement d'une autorité centrale de contrôle, le processus de validation des blocs peut s'avérer très long. Selon la complexité du calcul à résoudre pour valider le bloc et le nombre de transactions à la seconde, il peut prendre jusqu'à plusieurs dizaines de minutes[18]. La blockchain a été plutôt pensée comme une technologie de niche, et non d'échelle, et n'est pour le moment pas non plus adaptée à un usage « en temps réel ».

[16] https://www.20minutes.fr/arts-stars/culture/2283587-20180607-video-blockchain-bullshit-alle-visiter-ferme-bitcoins-secrete-islande
[17] https://digiconomist.net/bitcoin-energy-consumption
[18] https://siecledigital.fr/2017/03/20/blockchain-pas-si-simple-pour-les-grands-groupes

Cependant, cette consommation énergétique excessive et cette lenteur des transactions ne sont pas intrinsèques à la blockchain : ils dépendent essentiellement du mode de validation des transactions. Certains consensus s'avèrent plus efficaces et moins énergivores. A titre d'exemple, la « preuve de détention » (*proof of stake*) ne nécessite pas de puissance de calcul particulière puisque c'est un algorithme qui choisit les mineurs en évaluant leur possession d'actifs.

Toutefois, la consommation énergétique ou la puissance de calcul ne constitueraient pas des obstacles à l'utilisation de la blockchain par les Armées, puisque celle-ci passerait plutôt par une blockchain privée, c'est-à-dire ne nécessitant ni minage, ni consensus : c'est l'entité gouvernante -ici le ministère des Armées- qui prédéterminerait qui peut ou ne peut pas ajouter des blocs et consulter le registre. Le processus de validation serait alors plutôt basé sur la « preuve d'autorité » (*proof of authority*).

En revanche, l'usage de la blockchain dans les Armées, dans un contexte opérationnel, pourrait se heurter aux problématiques de l'encombrement ou de la faiblesse du réseau et des problèmes de connexion.

Capacité de stockage

Dans le cas où les blockchains servent à enregistrer non plus des transactions mais des documents (cas de suivi logistique ou de suivi RH par exemple), la question de la capacité de stockage se posera rapidement.

Une blockchain n'est effectivement qu'une base de données, grossissant à chaque bloc validé. L'augmentation du volume de données à traiter -et à transférer- s'accompagnera également d'un temps de transaction beaucoup plus long, ce qui réduira de fait l'efficacité opérationnelle de la chaîne.

L'augmentation du nombre de nœuds (participants) est également problématique dans le cas d'une blockchain de grande échelle, puisque plus

il y a de nœuds, plus il y a des transactions et de données à valider, et plus cela prend du temps, de la bande passante et de l'espace de stockage. La blockchain du bitcoin[19] pesait 105 Go en mars 2017, contre 90 Go trois mois plus tôt (+15%). Le bitcoin a été initialement créé pour réduire les coûts et les temps de transactions en s'affranchissant d'une autorité centrale, mais en prenant de l'ampleur, elle perd cette souplesse initiale. La blockchain Ethereum présente, dans une moindre mesure, les mêmes limites.

L'usage d'une blockchain privée résout une partie du problème puisque, comme vu précédemment, elle ne nécessite pas de minage ni de véritable consensus. Le nombre de nœuds est également contrôlé puisqu'une blockchain privée a vocation à être utilisée à une moindre échelle par rapport à une blockchain publique. En revanche, la question de la capacité de stockage dans le temps se pose réellement, car dans le cadre de la gestion des identités numériques et du suivi logistique, le volume de données enregistrées peut vite devenir très lourd et donc les transactions plus lentes. Une solution pourrait être l'utilisation de chaînes « latérales » ou « parallèles » (side-chains), qui permettent d'alléger le registre principal. Le concept de *side-chains* a été développé par la société américaine Blockstream[20]. Une *side-chain* est simplement « *une blockchain qui valide la donnée d'autres blockchains* »[21], c'est-à-dire qu'il y a échange de données/ d'actifs entre la blockchain principale et ses *side-chains*. En synchronisant les *side-chains* avec la chaîne principale (même règles de fonctionnement - validation, horodatage, etc.- et d'accès), il est alors possible d'augmenter la capacité de stockage du système global. Bien que reliées à la chaîne mère, les *side-chains* sont des entités bien distinctes : si, malgré leur inviolabilité théorique, une vulnérabilité apparaissait sur une *side-chain*, elle resterait cantonnée à celle-ci et ne viendrait pas « contaminer » la chaîne principale.

19 https://siecledigital.fr/2017/03/20/blockchain-pas-si-simple-pour-les-grands-groupes/
20 https://blockstream.com/technology/
21 https://blockstream.com/sidechains.pdf

Sécurisation des données et notion de confiance

La blockchain est une technologie encore très jeune et la prise de recul sur son efficacité réelle dans le long terme ainsi que sur les failles qu'elle pourrait révéler est encore limitée. Il est toutefois déjà possible de noter que, malgré les apparences, la blockchain n'est pas synonyme de sécurité absolue. Elle présente des vulnérabilités tant sur la chaîne elle-même (*on-chain*) qu'en dehors du système (*off-chain*). Quelques exemples (liste non exhaustive) :

On chain

Une blockchain publique est théoriquement vulnérable aux **attaques Sybil**[22]. Une attaque Sybil est la création par un individu de fausses identités dont il se sert pour influencer le réseau. Dans le cadre de la blockchain, l'individu malveillant crée différents nœuds « subversifs » et s'en sert pour prendre le contrôle d'une partie du réseau. La blockchain est alors corrompue et l'agresseur a accès aux données ou aux actifs contenus dans la chaîne. Notons que dans le cas de la blockchain Bitcoin, les attaques Sybil sont empêchées grâce aux « preuves de travail », qui rend les nœuds coûteux. Dans la cadre d'une blockchain privée, le risque d'attaques Sybil est limité. En effet, les nœuds qui valident les blocs sont connus et contrôlés par l'entité administrant la chaîne, ce qui -théoriquement- élimine de fait les nœuds malveillants. De plus, le nombre de participants est généralement bien plus réduit sur une blockchain privée que sur une blockchain publique, facilitant ainsi le contrôle des nœuds.

La blockchain présenterait également une vulnérabilité aux attaques **Man-in-the-middle** (MitM). Ces attaques sont « *une technique de piratage informatique consistant à intercepter des échanges cryptés entre deux*

[22] https://cdn.reseau-canope.fr/archivage/valid/feuilletage-les-risques-des-blockchains-N-11271-16257.pdf ; https://cdn.reseau-canope.fr/archivage/valid/feuilletage-les-risques-des-blockchains-N-11271-16257.pdf

personnes ou deux ordinateurs pour décoder les messages »[23]. L'initiateur d'une attaque MitM peut donc intercepter les transactions au sein d'une blockchain, voire même insérer des transactions invalides et les faire valider et ajouter aux blocs. Les attaques MitM représentent surtout un risque pour les blockchains publiques. Comme dans le cas des attaques Sybil, le contrôle des nœuds par l'autorité administrant une blockchain privée réduit, sans toutefois éliminer complètement, le risque de telles attaques sur une chaîne privée.

Off-chain

Si les informations contenues dans les blocs sont supposément sécurisées, se pose en revanche la question de la sécurité des canaux qui permettent à ces infos d'arriver à la blockchain, les **Oracles**[24]. La blockchain ne peut pas communiquer directement avec une source externe, car elle prend sinon le risque de se casser. L'Oracle remédie à cela en offrant à la blockchain un lien avec l'extérieur : il s'agit d'un programme informatique chargé d'insérer des données extérieures dans la blockchain. Les Oracles sont nécessaires pour la réalisation des « contrats intelligents » (*smart contracts*) : un *smart contract* est une transaction établie entre deux parties à un instant donné, mais qui ne sera réalisée qu'une fois les conditions préétablies vérifiées. Lorsque les conditions sont réunies, la transaction est déclenchée automatiquement au sein de la blockchain, sans intervention des parties impliquées et conformément aux conditions initiales. C'est donc l'Oracle qui va chercher à l'extérieur de la chaîne les données nécessaires à l'exécution du « contrat » et qui les intègre à la chaîne. Les Oracles sont en fait des sortes de tiers de confiance de substitution. Ainsi, il est important de pouvoir garantir leur sécurité et leur intégrités. Le programme peut en effet s'avérer être lui-même vulnérable à des attaques. Il peut aussi présenter des déficiences et

[23] https://www.futura-sciences.com/tech/definitions/informatique-attaque-man-in-middle-10048/
[24] https://www.ethereum-france.com/les-oracles-lien-entre-la-blockchain-et-le-monde/

empêcher ainsi le bon déroulement des « contrats » programmés. Enfin, il peut être malveillant et envoyer volontairement des informations erronées que la blockchain enregistrera définitivement dans un bloc. La chaîne se corrompra alors d'elle-même.

De la même façon, la question de la **sécurité des nœuds** se pose. Un individu connecté à la blockchain depuis son ordinateur n'est en effet pas à l'abri de diverses attaques (hack, DDoS, cryptolocker, etc.). Si un nœud est piraté, il peut être utilisé pour introduire des données erronées et ainsi corrompre la blockchain.

En conclusion…

En dépit de quelques limites, la blockchain semble présenter des caractéristiques indéniablement intéressantes pour la Défense française. Sa résilience, sa disponibilité et son inviolabilité en font un atout significatif pour différentes applications : messagerie sécurisée, gestion des identités et des fichiers RH, suivi logistique. C'est la notion de sécurité et d'immuabilité qui la rend particulièrement pertinente pour le domaine militaire.

Néanmoins, devant le manque d'études approfondies existantes, cette technologie doit bien évidemment être expérimentée et soigneusement évaluée avant d'être introduite dans le milieu de la Défense française. Si elle s'avérait finalement vulnérable, les conséquences seraient catastrophiques.

ceis

Société Anonyme au capital de 150 510 €

SIREN : 414 881 821 – APE : 7022 Z

Tour Montparnasse - 33, avenue du Maine - BP 36

75 755 Paris Cedex 15

Tél. +33 1 45 55 00 20 / Fax +33 1 45 55 00 60 / **contact@ceis.eu**

Publications récentes

A télécharger sur www.sia-lab.fr ou www.ceis.eu

Blockchain : état des lieux et perspectives - Janvier 2018

Internet des Objets (IoT) - Nouvelle donne pour la Défense ? – Juin 2017

Enjeux stratégiques du Big Data pour la Défense – Juin 2017

Emploi du Cloud dans les Armées – Juin 2016

Impression 3D - Technologie de rupture au service des Armées – Juin 2016

Rattrapages technologiques et technologies de l'information – Déc.2015

Impact de la numérisation sur l'exercice du commandement – Déc. 2015

Numérisation de l'outil de Défense – Juin 2015

Rythme des opérations et nouvelles technologies – Juin 2015

Mission des Armées et systèmes d'information – Déc. 2013

Le Système d'Information des Armées (SIA) – Déc. 2013

ceis