La *blockchain* est-elle un tournant stratégique ?

Olivier KEMPF | Consultant en stratégie digitale, directeur de la lettre d'analyse stratégique *La Vigie*. Il a publié avec François-Bernard HUYGHE et Nicolas MAZZUCCHI, *Gagner le cyberconflit, au-delà du technique* (Économica, 2015, 175 pages).

Les innovations informatiques se succèdent au point qu'il est difficile d'en prendre la mesure. Pourtant, chacun a pu apprécier l'importance de cette révolution informatique qui se déroule depuis maintenant 35 ans et qui avait été décelée très tôt par le jeune Zbigniew BRZEZINSKI (1971). Que se passe-t-il en effet ? Au cours des années 1980, les ordinateurs individuels se répandent : 1re vague de cette révolution informatique. Fin des années 1990, irruption d'*Internet* et de la communication entre ordinateurs : 2e vague. Milieu des années 2000, ce qu'on a appelé le *Web 2.0*, à savoir l'ère des *blogs* et autres réseaux sociaux permettant à tout un chacun de s'exprimer sur « la Toile » : 3e vague. Enfin, nous serions , au cours de notre décennie 2010, en train de vivre la 4e vague de cette révolution, celle que l'on dénomme « transformation numérique ».

Elle peut se caractériser par bien des choses : une très grande mobilité, des méthodes particulières, des outils nouveaux. Parmi ceux-ci, des mots reviennent : infonuagique (*cloud*), *Internet* des objets (*IOT*), Données massives (*Big Data*), Intelligence artificielle (IA), robotique, *blockchain* (« chaîne de blocs », en bon français, même si la traduction n'a jamais trouvé audience : nous accepterons donc *blockchain* dans cet article).

Celle-ci a attiré l'attention des grands médias à la suite de la spéculation autour du Bitcoin, une cryptomonnaie dont les cours se sont envolés cet hiver avant de replonger à des niveaux moins spéculatifs (mais toujours assez élevés *). Cependant, si le Bitcoin est indissociable de la *blockchain*, on ne peut réduire celle-ci aux cryptomonnaies. L'enjeu est différent et a des potentialités qui doivent intéresser les stratégistes.

Les généraux byzantins

Tout débute justement par un problème d'apparence stratégique, ce qu'on a appelé le dilemme des généraux byzantins. Peut-être faut-il y voir une allusion à

* Parti d'environ 5 000 $ à la fin de l'été 2017, il était monté au-dessus de 19 000 $ l'unité, puis il avait plongé fin décembre, baissant jusqu'à 6 500 $ début avril. Fin avril, il entamait une remontée autour de 9 500 $.

Bélisaire, le fameux général de l'empereur Justinien, résistant victorieusement aux Ostrogoths lors du siège de Rome en 537, ou peut-être aux assauts contre les Perses auxquels s'affrontait Byzance. Mais il s'agit surtout d'un problème mathématique de théorie des jeux décrit en 1982 par Leslie LAMPORT, Robert SHOSTAK et Marshall PEASE. Depuis les études sur la dissuasion nucléaire, les stratégistes ont appris quelques rudiments de théorie des jeux et ils liront donc ce qui suit avec plaisir.

Voici donc des généraux byzantins qui campent, chacun à la tête de son corps d'armée, autour d'une cité ennemie qu'ils assiègent. Ils ne peuvent communiquer entre eux qu'au moyen de messagers et c'est nécessaire pour établir un plan de bataille commun. Sans cette communication, la défaite sera certaine. S'il n'y avait que deux généraux, cela ne serait pas trop difficile mais imaginez que huit généraux assiègent le camp perse ? Chacun doit communiquer avec les sept autres et il n'y a pas de général en chef qui puisse assurer la coordination des huit.

Dès lors, tout repose sur les messagers. Que l'un d'eux soit un traître ou soit attrapé par l'ennemi, et les Byzantins perdent. Il a été démontré qu'en utilisant uniquement des messages oraux, ce problème des généraux byzantins peut être résolu, si et seulement si plus des deux tiers des messagers sont loyaux. Ainsi, un seul traître peut confondre deux généraux loyaux. De plus, le problème peut être résolu pour un nombre quelconque de messagers renégats si les messages sont écrits (et non falsifiables).

Bref, comment surmonter la défaillance d'un membre d'un groupe et établir un consensus suffisamment solide pour arriver à ses fins ? Comment établir la confiance dans un système décentralisé en partageant les intentions de chacun ? « La *blockchain* constitue la première et peut-être la seule solution au problème des généraux byzantins » (Laurent LELOUP, p. 46). Un système informatique décentralisé peut ainsi gérer les défaillances de certains de ses composants en utilisant un algorithme cryptographique fondé sur un système décentralisé de preuves. S'il existe d'autres systèmes de tolérance aux défaillances, la *blockchain* met l'accent sur un réseau de pair à pair et sur l'authentification cryptographique.

Ce problème aurait pu être réservé aux seuls informaticiens jusqu'à ce qu'un auteur écrivant sous le pseudonyme de Satoshi NAKAMOTO annonce en 2008 la naissance du Bitcoin, « une monnaie électronique fondée sur un système de pair à pair ». Par cette méthode qui résout le problème des généraux byzantins, deux agents peuvent échanger des actifs sans passer par un tiers de confiance.

Les cryptomonnaies ont popularisé la *Blockchain*

Le succès est rapide. Le Bitcoin est en effet une chaîne de blocs ouverte, « fonctionnant par un réseau de pair à pair, sans autorité centrale (et donc sans autorité financière [comme une banque centrale]) tout en enregistrant chaque

transaction (horodatage) dans un grand livre de compte (*ledger*) dans lequel toute modification est impossible » (L. LELOUP, p. 34).

Bitcoin, c'est donc de l'argent, ce qu'on appelle une cryptomonnaie : une monnaie, mais crypto, c'est-à-dire à la fois cachée (hors des banques centrales) et utilisant la cryptographie. Elle garantit ainsi la discrétion, grâce à une décentralisation absolue (celle du réseau pair à pair), mais pas l'anonymat, beaucoup moins que l'argent liquide par exemple (cf. RAY). Et c'est une monnaie car les transactions sont enregistrées « pour toujours ». Un actif reste un actif. Une chaîne de blocs constitue ainsi une technologie *WORO* (*Write Once, Read Only*) : on ne peut écrire qu'une fois l'écriture considérée sur le livre de compte : ensuite, il n'est possible que de la lire. D'ailleurs, chaque écriture est reliée à la précédente et ainsi de suite jusqu'au début : les écritures précédentes, authentifiées, garantissent la nouvelle écriture. Celle-ci n'est rendue possible que par la résolution d'un problème cryptographique (la preuve de travail, ou *Proof of Work*), opération que l'on désigne sous le terme de « minage » et qui nécessite de très grosses puissances de calcul.

Dans le cas du Bitcoin, chaque résolution de problème permet de gagner de nouveaux Bitcoins : cela explique pourquoi tant de consortiums se sont lancés dans le minage, pourquoi il y a des fraudes au minage (votre ordinateur peut être phagocyté pour participer en réseau à l'effort de minage), pourquoi enfin cela consomme énormément d'énergie. La folie du minage ressemble aux ruées vers l'or du XIX^{e} siècle. Toutefois, si l'or enrichit, le Bitcoin aussi ! Il se dit ainsi que Satoshi Nakamoto détiendrait un million de Bitcoins, soit près de 10 milliards de dollars… Il reste que le nombre de Bitcoins est limité : il y a un plafond à la masse monétaire en circulation.

À la suite du bitcoin, d'autres cryptomonnaies ont été lancées : on pense à Litecoin, Peercoin puis Monero, Ethereum, nouvelles cryptomonnaies utilisant des techniques supplémentaires (adresses de furtivité, contrats intelligents, etc.). Les systèmes de preuves évoluent également avec des calculs moins gourmands en énergie, mais aussi des possibilités nouvelles. Ethereum permet ainsi d'associer des contrats intelligents (*smart contracts*), technique qui est utilisée par certains assureurs dans des contrats expérimentaux : votre avion est annulé et automatiquement, par simple constat de l'annulation, la prime d'assurance vous est versée…

La folie des cryptomonnaies s'est étendue. Ainsi, Kodak a vu son cours de bourse multiplié par trois lorsqu'en janvier 2018, il a annoncé vouloir créer une cryptomonnaie Kodakcoin, liée aux échanges photographiques (voir l'article sur EGEA). La cryptomonnaie de la messagerie Telegram est attendue par beaucoup. De même, de multiples *start-up* proposent des *ICO* (*Initial Coin Offering*) : ce sont des systèmes permettant de financer les premiers capitaux propres grâce à la souscription des cryptomonnaies associées au projet de la *start-up*. Là aussi, il y a énormément de spéculation.

L'intérêt de la *blockchain* ne se limite pas aux cryptomonnaies

Est-ce pourtant à dire que la *blockchain* n'est qu'une affaire financière ? Non, car la cryptomonnaie n'est pas systématique et une chaîne de blocs est d'abord autre chose, selon Wikipédia : « Techniquement, il s'agit d'une base de données distribuée dont les informations envoyées par les utilisateurs et les liens internes à la base sont vérifiés et groupés à intervalles de temps réguliers en bloc, l'ensemble étant sécurisé par cryptographie, et formant ainsi une chaîne ». C'est un registre distribué (décentralisé) et sécurisé de toutes les transactions inscrites. Ces deux caractéristiques nous intéressent fortement.

Certains expliquent en effet que la *blockchain* revêt les caractéristiques du protocole *TCP/IP*, lorsqu'il apparut au milieu des années 1990 : qui eût parié sur la généralisation aussi massive de ce protocole qui a permis le développement d'*Internet* (et notamment la deuxième vague que nous mentionnions en introduction). Par beaucoup d'aspects, la *blockchain* permet de tels développements. Ses deux caractéristiques majeures sont en effet la sécurité et la décentralisation.

La sécurité intéresse par définition tous les stratégistes. Voici en effet un système garantissant des transactions de toute sorte, c'est-à-dire des échanges d'information. Or, une *blockchain* peut être utilisée de plusieurs façons : on parle ainsi de chaînes publiques, semi-publiques ou privées. Dans une chaîne publique, tout le monde peut écrire et lire. Dans une *blockchain* semi-publique, seuls les membres du consortium peuvent écrire mais tout le monde peut la lire. Dans une *blockchain* privée, seuls les membres du *consortium* peuvent écrire mais aussi la lire. Cette dernière configuration peut à l'évidence être utile pour de grandes organisations à multiples acteurs où le partage de l'information est difficile mais qui doit rester le fait des seuls membres : de ce point de vue, les organisations militaires sont particulièrement représentatives de ce cas de figure.

La décentralisation est cependant la caractéristique la plus importante. D'abord dans le monde civil. On dit en effet de la *blockchain* qu'elle peut ubériser Uber. Si l'industrie financière a été la première à prendre en compte l'impact potentiel de la *blockchain*, pour les raisons que l'on a vues, c'est toute l'économie qui risque elle aussi de se voir transformer en profondeur. On sait que la société Uber a fondé sa réussite sur l'intermédiation entre des offreurs de microservices (un voyage en stop, une chambre chez l'habitant) et des demandeurs. Ce modèle a été repris par de nombreuses plateformes : Uber donc pour les taxis, Blablacar pour le covoiturage, AirBnB pour les chambres chez l'habitant… Mais Uber et Blablacar se présentent comme des intermédiaires centraux qui gèrent l'intermédiation (et en tirent leurs profits). Or, une fois qu'on a compris que chacun pouvait acheter et offrir des microservices, a-t-on toujours besoin d'une plateforme dédiée ? Ne peut-on pas économiser les coûts associés à son usage ? Une *blockchain* totalement décentralisée permettrait de résoudre cette difficulté et donc de se passer d'Uber. La *blockchain* peut donc ubériser Uber.

L'intérêt stratégique pour la *blockchain* de par le monde

Constatons que dès 2015, les États-Unis se sont intéressés à la technologie de la chaîne de blocs dans une perspective de défense. La *DARPA* (*Defense Advanced Research Projects Agency*) a ainsi lancé en 2016 un appel d'offres pour une « plateforme de messagerie sécurisée » (cf. Giulio PRISCO) : celle-ci doit être capable de transférer des messages *via* un protocole décentralisé sécurisé sur plusieurs canaux, incluant le protocole de transport, le cryptage des messages et la mise en œuvre de la *blockchain* personnalisée.

La *DARPA* note que cette plateforme de messagerie sécurisée planifiée permettra de cartographier l'écosystème du ministère américain de la Défense (*DoD*), organisé actuellement selon une logique de métier qui entrave la bonne communication entre services. Outre une simplification des échanges, le système offre une meilleure sécurité et améliore la productivité. Selon le cabinet SIA PARTNERS, « la clé de chiffrement utilisée ne les rend lisibles que par le destinataire final, mais la diffusion du message crypté à l'ensemble du réseau garantit la stabilité du système de messagerie et la confidentialité des métadonnées, l'émetteur et le récepteur devenant impossibles à identifier par un tiers. Cela constitue 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 ».

À la suite de la *DARPA*, l'agence Otan des communications informatiques (la *NCIA*) a lancé un défi d'innovation sur ce même thème de la *blockchain*. Notons enfin que dans le programme de 700 milliards de dollars d'investissement de défense signé par le président Trump en décembre 2017, la *blockchain* est explicitement mentionnée dans la Section 1646 *.

Les Russes aussi sont intéressés, comme en témoigne la déclaration à l'agence *Tass* du PDG de Voentelecom (une société russe de télécommunications travaillant pour le ministère russe de la Défense) le 22 août 2017. En Israël, le principal fabricant d'aéronautique IAI a annoncé, en janvier 2018, développer un produit *blockchain* pour une solution de cybersécurité (cf. Shoshanna SOLOMON). La Chine ne semble pas en reste : on apprenait ainsi (cf. Wilson VORNDICK) que le colonel Zhu QICHAO, directeur du Centre des études stratégiques et de sécurité nationale de l'Université de défense et de technologie de Pékin, par ailleurs, un des experts chinois reconnus en Intelligence artificielle, avait coécrit un article en avril 2016 où il soulignait les intérêts de la *blockchain* dans la panoplie chinoise de sécurité. Il discernait ainsi trois domaines favorables : les opérations de renseignement,

* Le projet de loi décrit explicitement le cas d'utilisation de la technologie *blockchain* dans la défense nationale et l'applicabilité d'un registre immuable pour la protection des informations sensibles. L'étude devrait inclure une description des applications cyberoffensives et défensives potentielles de la technologie *blockchain* et d'autres technologies de bases de données distribuées ; une évaluation des efforts déployés par les puissances étrangères, les organisations extrémistes et les réseaux criminels pour utiliser ces technologies ; une évaluation de l'utilisation ou de l'utilisation prévue de ces technologies par le gouvernement fédéral et les réseaux d'infrastructures essentielles ; et une évaluation des vulnérabilités des réseaux d'infrastructures critiques aux cyberattaques (www.defense.gov/News/Special-Reports/0518_budget/).

le cycle de vie des armes et la logistique militaire. Toutefois, l'aspect structurellement décentralisé de la chaîne de blocs pose un évident problème au système centralisé chinois…

Quel intérêt militaire ?

On peut, d'ores et déjà, identifier plusieurs applications de la chaîne de blocs dans le monde de la défense. D'abord, des améliorations du fonctionnement organique.

La chaîne de blocs introduit en effet un changement de paradigme. Jusqu'à présent, les organisations et notamment l'institution militaire ont adopté une logique de château fort pour garantir l'information. Cette approche paraît de plus en plus vaine, tant l'information se multiplie et se disperse dans les usages les plus courants. Dès lors, utiliser une nouvelle technologie décentralisée est peut-être la bonne approche. Autrement dit, on passe d'un système vertical à un système horizontal, qui assure une meilleure résilience et surtout l'immuabilité de l'information qui y est déposée.

La chaîne de blocs permettrait alors une meilleure protection de nos informations, renforçant la cybersécurité actuelle. En effet, les menaces d'ordre cyber croissent exponentiellement (en nombre, en qualité et en diversité d'agression) et un nouveau modèle semble nécessaire. Premièrement, les réseaux *blockchain* sont conçus sans tiers de confiance (puisqu'il s'agit de répondre au dilemme des généraux byzantins), ils assument structurellement le compromis du réseau par les initiés et les étrangers. Deuxièmement, les *blockchain*s sont sécurisées de manière transparente et reposent sur une structure de données cryptographiques qui rend la falsification à la fois exceptionnellement difficile (attaque dite à 51 %, impossible à atteindre dans les faits) et immédiatement évidente. Enfin, les réseaux *blockchain*s sont tolérants aux pannes puisqu'ils mobilisent les efforts des nœuds valides pour rejeter ceux qui sont suspects. En conséquence, les réseaux de chaînes de blocs réduisent non seulement la probabilité de compromis, mais imposent également des coûts beaucoup plus élevés à un adversaire pour l'atteindre. Un des objectifs recherchés par la *DARPA* serait donc de garantir l'intégrité des données associées à des systèmes d'armes cruciaux, comme ceux soutenant les armes nucléaires ou les satellites (cf. Joon Ian WONG).

Notons enfin que la *blockchain* sera probablement le meilleur moyen de contrôler la sécurité de l'*Internet* des objets (*IOT*) dont les déficiences sont aujourd'hui patentes. Le logiciel malveillant Mirai a ainsi utilisé un réseau de caméras de surveillance pour susciter une des plus grandes agressions DDOS (attaque par déni de service) de l'histoire, en septembre 2016. Or, la sécurité informatique de la plupart de ces objets est défaillante. Placer un réseau d'objets connectés sur une *blockchain* permettrait sans nul doute de contrôler les échanges entre eux, d'autant

plus que la chaîne gagne en sécurité à mesure que des organisations s'y connectent. Une expérience britannique aurait ainsi été menée en ce sens avec le *Defence Science and Technology Laboratory* (*DSTL*), la DGA d'outre-Manche : « *using a blockchain to improve the trustworthiness of a network of sensors on, for example, security cameras* ».

Mais la *blockchain* pourra également améliorer les opérations. Cela paraît évident en termes de logistique, un des grands domaines civils où elle se répand à grande vitesse. La chaîne de blocs permet ainsi d'accélérer les livraisons, d'améliorer la qualité des produits en flux tendu ou encore de faciliter la maintenance des véhicules. De même, elle permet de garantir la traçabilité des denrées et produits transportés. On imagine la fiabilité obtenue dans les acheminements opérationnels de logistique diverses vers des zones les plus difficiles et dans des environnements inconfortables (Tchad, Mali, Afghanistan). L'auteur de ces lignes se souvient ainsi d'un conteneur de pièces de rechange qui avait disparu et qui empêchait le Maintien en condition opérationnelle (MCO) des bataillons déployés à Abéché lors de l'opération *EUFOR Tchad*. On l'avait retrouvé, dix mois après, égaré dans une zone de stockage annexe.

Comme le constate le cabinet Sia Partners, « la possibilité de mieux gérer les acheminements de matériels *via* la *blockchain* devrait permettre selon IBM une réduction de 20 % des coûts grâce à la réduction des démarches administratives et des erreurs, la réduction des temps de transit sur toute la chaîne d'approvisionnement et la simplification des processus. [Elle] devrait aussi permettre une diminution des coûts d'assurance en offrant un meilleur contrôle aux clients sur les transports de leurs marchandises. La *blockchain* permet aussi de résoudre de nombreuses difficultés actuelles : les contrôles et les vérifications sont réalisés par consensus et chaque étape est scrupuleusement enregistrée. Cette technologie permet ainsi de diminuer les coûts des opérations de vérification, et plus généralement du *tracking* ».

D'autres apports opérationnels peuvent être imaginés, plus proches des missions des troupes de contact : le contrôle des armes à feu dans la circonstance de processus DDR (Désarmement, démobilisation et réintégration) ou encore la certification du statut et du niveau de sécurité des individus accédant à une base opérationnelle.

⁂

En quelques mots, la *blockchain* présente plusieurs qualités qui intéresseraient la défense : une source unique et immuable d'authenticité des informations qui y sont enregistrées ; l'organisation plus facile et plus visible de chaînes logistiques complexes ; un système automatisé ; une qualité de service renforcée ; un meilleur système de compte rendu, donc de pilotage ; une sécurité renforcée ; et surtout, un chemin privilégié vers la transformation digitale qui est synonyme de décentralisation, mobilité et explosion du nombre de données, autant de contraintes auxquelles la chaîne de blocs répond avec aisance.

À l'heure où l'intelligence artificielle est dans toutes les bouches et fait l'objet de toutes les attentions, la chaîne de blocs constitue une innovation technologique probablement plus accessible et aux potentialités certaines. La négliger serait une erreur.

Éléments de bibliographie

Brzezinski Zbigniew, *La révolution technétronique*, 1971, Calmann-Lévy (1970 pour l'édition anglaise).

Kempf Olivier, « Kodak et le numérique : naufrage puis renaissance », *EGEA Blog*, 28 avril 2018 (www.egeablog.net/index.php?post/2018/04/28/Kodak-et-le-num%C3%A9rique%3B-naufrage-puis-renaissance).

Lamport Leslie, Shostak Robert et Pease Marshall, « The Byzantine Generals Problem », *ACM Transactions on Programming Languages and Systems*, vol. 4, n° 3, juillet 1982.

Leloup Laurent, *La* blockchain, *la révolution de confiance*, Eyrolles, 2017, 224 pages.

Lian Lin, Zhu Qichao et Zhao Zhao, « Blockchain Technology and Its Potential Military Value [区块链技术及其潜在的军事价值] », National Defense Science & Technology [国防科技], vol. 37 n° 2, avril 2016, p. 30-34.

Nakamoto Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008 (https://bitcoin.org/bitcoin.pdf).

Prisco Giulio, « DARPA, NATO Looking at Military Applications of Blockchain Technology », *Bitcoin Magazine*, 23 mai 2016 (https://bitcoinmagazine.com/).

Ray, « Bitcoin : le point sur l'anonymat », *Contrepoints.org*, 20 juin 2014 (www.contrepoints.org/2014/06/20/169540-bitcoin-le-point-sur-lanonymat).

Sia Partners, « La *blockchain*, nouvelle botte secrète des armées », 1er mars 2018 (http://secteur-public.sia-partners.com/20180301/la-blockchain-nouvelle-botte-secrete-des-armees).

Solomon Shoshanna, « Bank Hapoalim IAI to join forces on using blockchain for cybersecurity applications », The Times of Israel, 3 janvier 2018 (www.timesofisrael.com/bank-hapoalim-iai-to-join-forces-on-using-blockchain-for-cybersecurity/).

Tass, « Blockchain Technology may be introduced in Russia's Armed Forces », 22 août 2017 (http://tass.com/defense/961423).

VornDick Wilson, « Beyond Bitcoin : Could China Embrace Blockchain for Defense and Security Applications ? », *China Brief*, vol. 18, n° 2, The Jamestown Foundation, 13 février 2018 (https://jamestown.org/program/beyond-bitcoin-china-embrace-blockchain-defense-security-applications/).

Wong Joon Ian, « Even the US military is looking at blockchain technology—to secure nuclear weapons », *Quartz*, 10 octobre 2016 (https://qz.com/).