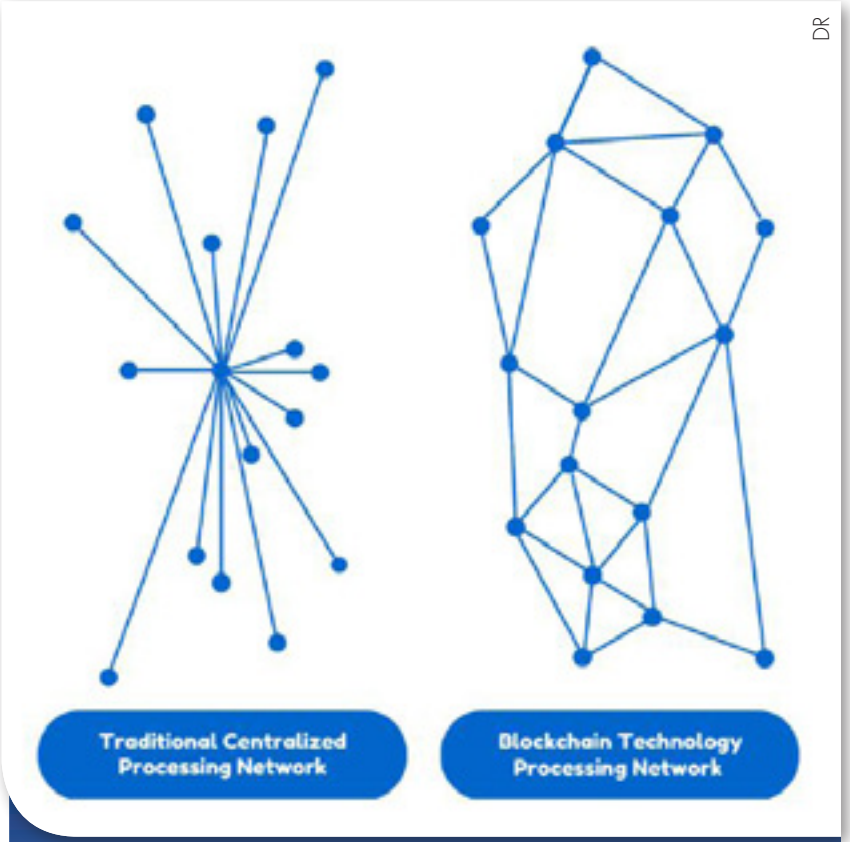
Comprendre la technologie blockchain Quelles applications dans la défense ?



La blockchain : du centralisé au décentralisé.

La blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée et fonctionnant sans organe central de contrôle. Par extension, une blockchain constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne.

Il existe des blockchains publiques, ouvertes à tous, et des blockchains privées dont l'accès et l'utilisation sont limitées à un certain nombre d'acteurs. Une blockchain publique peut donc être assimilée à un grand livre comptable public, anonyme et infalsifiable. Comme l'écrit le mathématicien Jean-Paul Delahaye, il faut s'imaginer « *un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible* ». Si cette technologie est apparue avec la crypto-monnaie, connue sous le nom de *bitcoin*, son architecture intéresse aujourd'hui de nombreux acteurs dans le cadre de multiples applications.

Le transfert d'actifs

En premier lieu, dans le domaine des applications purement civiles, la blockchain permet le transfert d'une valeur monétaire entre 2 entités sans avoir recours à un tiers de confiance, diminuant ainsi le coût lié à cette transaction. Si traditionnellement, le transfert de monnaie se fait par le biais d'un intermédiaire rémunéré par lequel transite ce flux, la blockchain permet de s'en affranchir (avec un coût globalement 9 fois inférieur à celui pratiqué par les établissements traditionnels…) et d'aboutir au même résultat de manière plus sécurisée. Les transferts de bitcoin ne prennent théoriquement que quelques minutes : le temps nécessaire à la validation du bloc et à son intégration dans la chaîne bitcoin.

La tenue de registres

Les blockchains sont de véritables *livres de comptes* qui enregistrent l'ensemble des informations traitées et validées d'un service donné. Ces informations sont réputées infalsifiables. Le virement d'une crypto-monnaie, par exemple, entraîne systématiquement l'enregistrement de l'ensemble des informations relatives aux utilisateurs et aux transactions. Cette propriété permet une grande transparence dans les échanges entre les utilisateurs car l'ensemble des transactions est partagé et enregistré par le réseau.

Quand le Pentagone s'intéresse à la blockchain

La Defense Advanced Research Projects Agency (DARPA) a publié un appel à projet pour créer une messagerie chiffrée totalement décentralisée grâce à la technologie de la blockchain.

Contrairement aux forces de police qui songent à insérer des *portes dérobées* dans les messageries sécurisées, la DARPA envisage une messagerie ultrasécurisée, impossible à pirater et facile à utiliser, tant sur le web qu'à l'aide d'un smartphone. Celle-ci utiliserait des mécanismes de chiffrement sophistiqués, comme ceux de Signal ou WhatsApp, tout en s'appuyant sur une infrastructure décentralisée. Concrètement, les messages seraient chiffrés puis postés sur un registre de type blockchain. Ils seraient donc accessibles à tous, mais lisibles seulement par le destinataire qui détient la clé de déchiffrement.

Les avantages d'un tel système sont multiples. Tout d'abord, il serait très résilient, car il n'y aurait pas de serveurs centralisés dédiés à l'acheminement, qui constituent généralement une cible privilégiée pour les hackers. Par ailleurs, un tel système rendrait la surveillance plus difficile, car il déconnecte totalement la phase de création du message de sa phase de lecture. Comme tous les utilisateurs ont accès à tous les messages, il serait difficile de savoir à qui les messages étaient destinés.

Sur le fond, ce principe d'une diffusion *broadcast* de messages chiffrés n'est pas totalement nouveau. Il a été utilisé dans certains groupes de discussion « *anonymous* » en conjonction avec l'algorithme de chiffrement PGP. Ce principe est également appliqué dans des développements plus récents comme BitMessage, un protocole de communication décentralisé et chiffré destiné à permettre d›échanger des messages chiffrés. Mais l'originalité du projet de la DARPA est de faire appel à la technologie blockchain.

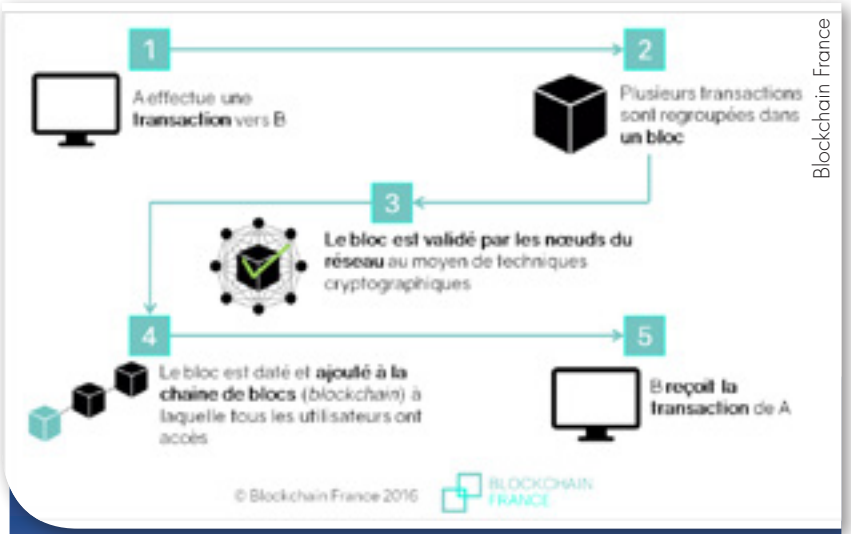
Toutefois, avoir des millions d'utilisateurs est très compliqué. Cela pose aussi des difficultés concernant les utilisateurs mobiles qui n'auront pas forcément accès à une bande passante suffisante, la puissance de la batterie et l'espace disque nécessaire pour traiter de grands volumes de données en permanence.

Le projet devrait se dérouler en 3 phases, sans plus de précision calendaire. Dans un premier temps, il s'agira d'élaborer un modèle théorique, puis de créer un prototype, enfin de procéder à la mise en œuvre finale de la technologie.

La disponibilité du code source de la technologie blockchain a permis le développement de nouveaux types de blockchains adaptées aux besoins des entreprises et des gouvernements. Exemple le plus connu, le Honduras a adopté un registre de titres fonciers basé sur la blockchain. L'enjeu pour le pays étant de développer un registre infalsifiable qui comporte l'ensemble des informations de propriété des citoyens.

Les *smart contracts*

Ce sont des applications destinées à répondre à un besoin de sécurité, de confiance et de transparence. La différence entre ces derniers et les contrats classiques réside dans le fait de pouvoir faire confiance au *code informatique* en lieu et place d'un tiers de confiance *traditionnel*. Les *smart contracts* peuvent être définis comme un programme informatique qui exécute des tâches après la vérification de conditions préalablement définies. Contrairement à la blockchain bitcoin, dédiée uniquement aux transactions financières, le champ d'application des *smart contracts* est très large et concerne de nombreux secteurs d'activité, avec d'immenses bouleversements à la clef, mais qui sont encore mal appréhendés.



Le fonctionnement d'une blockchain.

Blockchain et contrôle aux frontières : l'exemple de Dubaï

Une start-up britannique vient de signer un contrat avec Dubaï pour permettre aux voyageurs qui arrivent à l'aéroport de Matar Dubaï al Dawlyy de récupérer leurs bagages sans avoir à passer par la douane pour vérifier leur passeports. S'appuyant sur la technologie blockchain, les vérifications des passeports et des visas seront automatisées, l'échange de données étant mis en place lors de l'achat du billet. Les informations seront stockées sur de nouveaux passeports numériques.

Dubaï ambitionne de devenir un leader mondial dans l'utilisation de la technologie blockchain et de l'internet des objects (IoT) d'ici 2020.

Un peu d'histoire

L'être humain a pour habitude de vivre en groupe, avec comme corollaire de pouvoir effectuer des transactions.

Jusqu'au XVII^{e} siècle le modus vivendi est le troc, puis des monnaies sont battues et des unités de compte interopérables mise en place. Apparaissent ensuite les valeurs fiduciaires, où la valeur est détachée du support physique, jusqu'à l'époque actuelle avec la digitalisation des moyens de paiement.

Parallèlement, au siècle des Lumières, la notion de propriété se développe. La consolidation des États européens favorise la création des premiers registres nationaux. Ainsi, sous Napoléon, le cadastre répond au besoin d'un document de référence, digne de confiance et utilisable lors des transactions entre particuliers.

La confiance est le cœur de la monnaie fiduciaire, car contrairement à une pièce de métal (or, argent…), la valeur intrinsèque d'un billet de banque est nulle. Pour créer cette confiance, les monnaies doivent être adossées à des institutions (villes, puis États puis organisations internationales). Un tiers de confiance est donc indispensable au développement de la monnaie et de la propriété.

Après la Seconde Guerre mondiale, l'augmentation des transactions à l'international va demander de faire appel à de nouveaux tiers de confiance, comme le système interbancaires SWIFT. La mission de ces tiers est alors double : apporter les conditions d'un échange sécurisé et fluide, et au moindre coût.

En 2008, Satoshi Nakamoto, la mystérieuse figure (toujours inconnue à ce jour) derrière l'invention du bitcoin, publie Bitcoin : A Peer-to-Peer Electronic Cash System. Il y expose une méthode pour résoudre un problème cryptographique sur lequel butait la recherche depuis plusieurs décennies, le problème du double paiement. Celui-ci empêchait à 2 agents d'échanger des actifs, comme une monnaie par exemple, sans le passage par un tiers de confiance. La solution repose sur l'architecture décentralisée qui supporte bitcoin : la chaine de blocs, ou blockchain. Cette découverte est historique dans la mesure où elle autorise ce qui était auparavant impossible : 2 agents qui ne se connaissent pas peuvent échanger des actifs sans que la transaction ne doive être sécurisée et validée par une autorité centrale.

Le premier type de transaction a été le bitcoin, mais Sathoshi Nakamoto prévoyait l'extension du champ d'application. Ainsi, l'ensemble des actifs nécessitant un bureau central pour être échangés peuvent a priori être disruptés par la technologie blockchain : actifs, titres de propriété… Mais la puissance de la blockchain ne se réduit pas à des transactions statiques, les contrats passés pouvant inclure des variables, comme la performance par exemple. Le contrat devient donc intelligent et capable d'opérer seul, sans institution de référence… Plusieurs contrats pouvant s'articuler les uns aux autres autour de règles communes, avec la mise en place de gouvernances totalement nouvelles…

Blockchain publique et blockchain privée

La technologie Blockchain est adaptable : le degré d'ouverture d'une blockchain peut être limité pour créer une blockchain dite *privée*. Ce modèle s'oppose aux blockchains *publiques* comme celle à l'œuvre derrière bitcoin, que n'importe qui peut consulter et utiliser.

La situation est comparable à celle du réseau Internet où des intranets privés cohabitent avec l'Internet public : le débat blockchain publique/privée lie à la fois questions idéologiques et enjeux techniques.

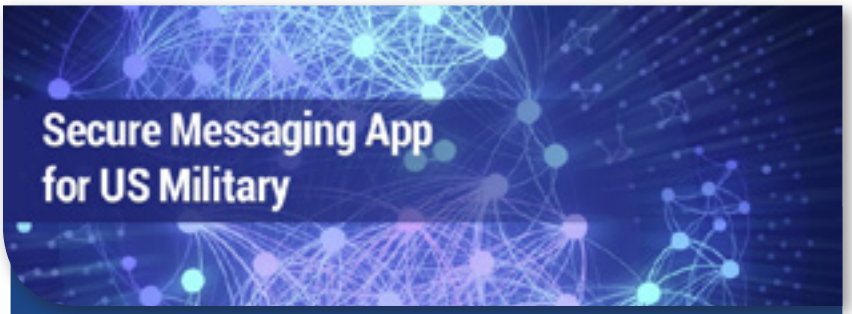
Des applications possibles pour la défense

Le panorama des usages potentiels au sein de la défense est double. Celui du monde civil bien entendu, par simple effet de transposition : signatures électronique de documents, règlement de fournisseurs une fois une prestation réalisée, contrôles d'accès, économies d'énergie, registres fonciers (le ministère des Armées est le deuxième propriétaire foncier de France…), votes à distance (syndicats, organismes consultatifs…) mais également mise en œuvre d'imprimantes 3D, par exemple à bord d'un navire, etc…

Dans les domaines spécifiques à la défense, l'utilisation de blockchains privées et cryptées peuvent notamment permettre l'enregistrement et le partage de données ayant un besoin d'intégrité extrême (plans d'opérations, *ciblage*, règles d'engagement, plans d'infrastructures sensibles…) ou à fort besoin de traçabilité (suivi des effectifs, de l'armement… mais encore de la situation logistique en opérations, ou des configurations informatiques).

Plusieurs limites pourraient toutefois freiner de tels développements : la taille des blocs de la chaîne, le débit du réseau (et donc sa rapidité), l'impossibilité à fonctionner en mode déconnecté, et enfin le coût des infrastructures nécessaires.

Fort à la mode, le terme de *disruptif* s'applique à la blockchain, technologie dont l'invention est sans doute comparable à celle d'Internet et qui devraient entraîner des bouleversements notables (pour ne pas dire cataclysmique) dans certains secteurs (métiers de banques, notaires, cadastre…) qui reposent encore sur la notion de *tiers de confiance*.



La technologie blockchain s'applique potentiellement à la défense. Le Pentagone cherche notamment à développer une messagerie ultra-sécurisée, impossible à pirater et facile à utiliser, sur le web, avec un simple smartphone (cf. encadré 1).

Technologie duale, elle ouvre à terme de nouveaux horizons dans le domaine de la défense, en alliant efficacité renforcée et agilité.

Patrice Lefort-Lavauzelle

Pour aller plus loin :

Bitcoin : A Peer-to-Peer Electronic Cash System, Bitcoing.org
Big bang blockchain, Stéphane Loigon, Tallandier.
Comprendre la blockchain, Livre blanc édité par U.
Les applications de la blockchain, Lettre mensuelle de l'OMC n° 50 (DGRIS).

Un plan d'opération. Partage de données et besoin d'une intégrité extrême : les atouts de la blockchain privée et cryptée.