La *blockchain*, au service de la sécurité

Par Jacques Favier & Élie Fontana,
avec la participation d'Édouard Klein

Blockchain: pourquoi l'Armée?

Pourquoi faudrait-il qu'aux côtés des nuées de start-ups qui depuis des années promettent monts et merveilles "grâce à la *blockchain*", les Armées manifestent de l'intérêt pour ce sujet né tellement loin des préoccupations militaires? La *blockchain* n'est-elle pas le nom forgé pour singer *Bitcoin* sans citer son nom, voire sans parler de "monnaie" parce qu'il était entendu que le sujet de la monnaie était une chasse jalousement gardée?

Mais comme l'argent est le nerf de la guerre, et que *soldat*, *solder* et *sou* ont même racine latine, les auteurs pensent qu'il y a au contraire nombre de bonnes raisons non seulement pour que les militaires s'informent de ce que les *blockchains* permettent, mais aussi pour qu'ils investissent ce terrain très particulier du cyberespace.

L'armée et la monnaie

On crédite toujours les seuls gens de finance de l'invention du papier monnaie. Pourtant, en France, bien avant le dérapage de l'expérience de Law, de nombreux billets destinés à remplacer les monnaies métalliques souvent insuffisantes étaient créés par divers corps de l'État, mais aussi de l'Armée: à côté des billets des Caisses des Gabelles, des Emprunts, ou des Fermiers Généraux, on trouvait ceux des États-Majors, de l'Extraordinaire des Guerres, de la Marine, ou de l'Artillerie. Et puis...le créateur de la Banque de France n'était-il pas artilleur?

En rester à ces utiles rappels serait cependant superficiel. L'intérêt réciproque, avant comme après la Révolution, entre gens de guerre (et tout spécialement de l'artillerie) et gens de monnaie tient à une chose: le bronze. Il y a une histoire fascinante[1] des enrichissements réciproques entre ces deux mondes, sur la technique métallique, les alliages, etc. Rappeler cela n'est pas anecdotique. À cette époque, la monnaie était faite de métaux rares et stratégiques. Ceux qui reprochent aux monnaies des *blockchains* d'être consommatrices d'énergie, de puissance de calcul ou d'espace de stockage ne voient simplement pas qu'il s'agit de l'or, de l'argent et du bronze numérique. La *blockchain* est stratégique.

Plus concrètement, l'armée s'est vue parfois contrainte de prendre le relais des autorités monétaires dans des situations particulières, qu'on appelle savamment "obsidionales". Et là, c'est toute l'histoire des "monnaies de siège" qu'il faudrait évoquer.

En 1521, les troupes françaises assiégées dans Tournai par celles de Charles-Quint battent une très éphémère monnaie qui portait au revers l'explicite légende: *moneta in obsidione tornacensi cusa*. Ce serait au siège de Leyde par les Espagnols en 1574 qu'aurait été *imprimée* la première monnaie de siège, sur du papier arraché aux livres de messe parce

[1] *Cf.* https://journals.openedition.org/ahrf/154.

que tout le cuir avait déjà été bouilli et mangé. Oublions le débat d'experts pour savoir si de tels *ersatz* sont encore des pièces ou déjà des billets et concentrons-nous, non sur la nature mais sur la circonstance de leur émission.

Alors que l'impression des premiers billets fiduciaires (*Bank of England*, assignats) fut un acte de *politique* monétaire, la monnaie obsidionale est un acte d'*administration* : "à la guerre comme à la guerre". Faute d'argent, les troupes françaises assiégées dans Anvers en 1814 frappèrent du bronze, du cuivre, du plomb et même du laiton. Il ne faut pas s'attacher à la matérialité, mais d'abord noter que la monnaie de siège reste une monnaie d'État ou du moins une monnaie autoritaire. La guerre, *continuation de la politique* selon Clausewitz, est une situation politique dans laquelle il n'y a pas défaut mais, pourrait-on dire, trop-plein de puissance. D'où le détail amusant de ces monnaies d'Anvers : les premières furent frappées à l'avers du *N* impérial, les dernières, après l'abdication à Fontainebleau, du monogramme de Louis XVIII. On ne toucha pas au revers...

L'armée et les transmissions

La cryptographie, sans laquelle il n'y aurait point de *blockchain*, est aussi un domaine qui intéresse depuis toujours les militaires. L'un des premiers chiffres par substitution ne porte-t-il pas le nom "chiffre de César" tandis que le chiffrement par transposition servait déjà, avec la scytale, aux généraux lacédémoniens? Or, si l'on chiffre l'information, c'est aussi qu'on la transmet. Et cette transmission est elle-même une arme.

La transmission a été désignée comme "l'arme qui unit les armes". Au tambour puis au clairon, à la trompette dans la cavalerie, avec des pavillons de transmission en mer, par estafette, et naturellement par télégraphe, puis téléphone ou par voie hertzienne, l'information doit être transmise pour réduire le "brouillard de guerre".

À chaque fois, le message peut être en clair ou avoir besoin de chiffrage, mais il a toujours besoin d'une infrastructure pour être distribué au loin. Plus encore que le fourrage ou les munitions, dont Clausewitz rappelle que les armées françaises se fournissaient largement "chez l'habitant", la poste militaire demande une infrastructure d'une extrême sophistication et d'une grande résilience. Le directeur général des postes de Napoléon était un officier, Lavalette, proche de lui depuis Arcole.

Avant l'avènement du fil, l'imagination se déchaîne autour des transmissions optiques. Elles apportent une information stratégique pour les stratèges comme pour les banquiers (même si l'histoire de Nathan Rothschild profitant avant les autres de Waterloo pour faire fortune est sans doute mythique) et offrent des failles aux pirates, ce qui inspira Alexandre Dumas.[2]

Avec le fil vient le Morse (1832), dont proviennent en ligne directe les compagnies Western Union et AT&T. Transporter l'information ou l'argent est une activité stratégique. Depuis la forteresse du Mont Valérien, les sapeurs télégraphistes et leurs descendants vont prendre toute leur part à la guerre moderne. Un jour, c'est par la voie hertzienne que circuleront, avec l'information, les mots "Honneur et Patrie" traçant la voie de la résistance.

---

[2] *Cf.* http://telegraphe-chappe.com/chappe/Litterat/dumas.html.

Mais au titre des *servitudes et grandeurs militaires,* on a vu maintes fois l'Armée déployée en supplétive des civils, pour sa capacité logistique (transporter les personnes, des vivres, des médicaments, voire des ordures ménagères...) et l'on sait que la logistique, rebaptisée *supply chain* dans le jargon start-up, est l'un des domaines où la mise en œuvre d'une *blockchain* est vantée pour ses vertus en termes de fiabilité, d'automaticité, de traçabilité.

L'armée et la confiance: les généraux byzantins

La *blockchain* est souvent décrite comme un instrument permettant de se passer du "tiers de confiance". C'était clairement le projet de *Bitcoin*: échapper à la prédation des banques et au contrôle des États et, les écritures étant protégées par un rigoureux pseudonymat, sans obligation déclarative, placer les transactions et l'intégrité des soldes sous le seul contrôle d'une communauté ouverte d'utilisateurs encadrés par la solidité d'un algorithme de consensus.

C'est moins nettement le cas avec les *blockchains* dites "privées" où un tiers attribue, ou non, la fonction de validateur des écritures ou l'accès aux données. Mais dans tous les cas, l'essor des contrats auto-exécutables (les *smart contracts*) ne peut guère se faire sans apparition de nombreux "oracles" en fonction desquels lesdits contrats s'exécutent en faveur de l'une ou de l'autre des parties. Même mécaniques et automatisés (un thermomètre, ou un compteur de vitesse…) ces oracles réintroduisent une fonction de "confiance". Comme cela a été écrit par ailleurs,[3] la fonction de "tiers de confiance" est sans doute moins menacée dans son essence que dans ses monopoles actuels.

Que l'armée soit un possible "tiers de confiance" ne fait pas l'ombre d'un doute. Le baromètre de la confiance politique de janvier 2019[4] la plaçait au premier plan, avec 21% de français "très confiants", devant la police (17%). En tenant compte des "plutôt confiants" les deux institutions étaient à 74%, à égalité avec… les PME, et seulement dépassées par les hôpitaux (78%). La crise des "gilets jaunes" a conforté l'armée (+2% dans le sondage 2020[5]) et sévèrement affecté la police (–8%) sans même entrer dans la problématique de la très inégale perception de la police sur l'ensemble du territoire.

Pourtant l'armée est elle-même une institution "méfiante", tout l'art de la guerre reposant, selon Sun Zu, sur la tromperie. Tant et si bien que lorsque en 1982 Leslie Lamport, Robert Shostak et Marshall Pease voulurent donner un nom percutant au problème ardu de l'établissement d'un consensus décentralisé, ils imaginèrent une scène guerrière : différents "généraux byzantins" doivent établir un plan de bataille pour envahir un camp ennemi, mais ne peuvent communiquer qu'à l'aide de messagers, alors même que certains généraux peuvent être des traîtres et que des messagers peuvent être corrompus.

Que ces "généraux byzantins" fassent allusion à un fait historique obscur ou que l'un des auteurs ait eu une réminiscence de cinéphile, songeant à *Theodora, impératrice de*

---

[3] Jacques Favier & Adli Takkal-Bataille, *Bitcoin, la monnaie acéphale*, Paris, CNRS, 2017, pp.47 et 234.

[4] *Cf.* http://www.sciencespo.fr/cevipof/sites/sciencespo.fr.cevipof/files/CEVIPOF_confiance_vague10-1.pdf.

[5] Voir : http://www.sciencespo.fr/cevipof/sites/sciencespo.fr.cevipof/files/OpinionWay%20pour%20le%20CEVIPOF-Barome%CC%80tre%20de%20la%20confiance%20en%20politique%20-%20vague11%20-%20Comparaison-1.pdf.

Byzance (1954) ou au *Dernier des Romains* (1967), n'a aucune importance pour nous. Ce qui compte, là encore, c'est que la *blockchain* est stratégique : qu'elle concerne donc les armées.

La technologie des protocoles à *blockchain* est née d'Internet, et Internet est né de l'Arpanet, de la DARPA. Le rôle joué aux États-Unis par cette Agence pour les projets de recherche avancée de défense est trop connu pour que l'on y insiste, sinon pour souligner que, du Darpanet devenu Internet au réseau en oignon (TOR), les militaires américains ont souvent fait le pari de la décentralisation, de la distribution et de l'anonymat. La DARPA a d'ailleurs annoncé en juillet 2019 son intention d'utiliser une *blockchain* pour sécuriser certaines transmissions.

L'objet du présent article est d'examiner ce qui se fait, en matière de *blockchain*, en France et dans plusieurs armées de pays alliés ou non. À l'heure où il est rédigé, ses auteurs ont la conviction que la crise née de la pandémie du coronavirus, du confinement d'une moitié de l'humanité, des chocs sanitaires, psychologiques, financiers, politiques et peut-être des confrontations stratégiques qui vont s'ensuivre, plaide pour un intérêt accru des spécialistes de la sécurité et de la défense envers une technologie informatique porteuse d'une forme particulièrement *résiliente* d'ordre.

Aperçu sur la *blockchain*

Court historique

Bitcoin, *un assemblage génial*

À tous ceux qui expliquent que le "sulfureux bitcoin" fonctionnerait bien mieux une fois ôté ceci ou cela, il importe d'expliquer qu'il s'agissait non d'une découverte, que l'on pourrait décliner, mais d'un génial assemblage: la notion de "pair à pair", la fonction de *hashage* cryptographique, la cryptographie asymétrique, le registre distribué et structuré en arbre de Merkle, tous ces éléments préexistaient (parfois depuis longtemps) à la publication de Satoshi Nakamoto en novembre 2008. En isoler un élément (le registre distribué, le plus souvent) ne perfectionne pas l'assemblage, il ramène simplement l'invention en arrière dans le temps, vers la boîte à outils.

L'histoire de *Bitcoin* s'enracine dans l'histoire de l'Internet. Celui-ci, dès son origine, cherchait sa monnaie native, son cash. Malgré les prétentions des banques à être des géants du numérique, chacun sait bien que l'on peut envoyer un message ou une photo en un instant, organiser une conférence en vidéo sur trois pays en quelques secondes, mais qu'il faut des heures pour envoyer dix euros à Bruxelles.

L'idée courait donc depuis longtemps de *simplifier* en s'inspirant de l'argent liquide, dont le transfert, ne requérant aucun intermédiaire, se fait instantanément. Le génie de l'inventeur de *Bitcoin*, fut là encore dans la simplicité: en renonçant à transférer des dollars (qu'en fin de journée il fallait bien solder en banque, ou dans un pot commun centralisé) et en décidant de transférer des unités de compte propres au jeu lui-même, non seulement il achevait de résoudre la quadrature du cercle (un paiement sécurisé sans teneur de compte centralisé) mais, par une décision proprement "souveraine", il créait une monnaie nouvelle. Ce jeton, qui n'était en vérité qu'une série d'écritures de transferts

cristallisées par une dépense énergétique importante, était aussi le premier objet non-copiable apparu dans le monde numérique.

Lui donner une "vraie valeur" en instituant la *même* unité de compte comme monnaie de rétribution des validateurs, organiser la rareté de ladite monnaie… tout ceci achève de donner au concepteur inconnu la figure de l'un des génies du temps.

Le buzz blockchain*, entre* uberisation d'Uber *et missile anti-GAFAM*

Pour enlever son venin à la chose, les grandes figures du monde de la finance organisèrent un brouillard épais d'approximations catégoriques et de non-sens péremptoires. Dès l'automne 2015 se répandit, à la suite d'une interview de Blythe Masters (déjà inventrice des produits mis en cause dans la crise de 2008) et d'un numéro spécial de *The Economist* présentant la *blockchain* comme "*The trust machine*", l'idée que celle-ci allait rendre d'incroyables services dépassant de très loin cette chose sans intérêt qu'est le paiement.

Les promesses furent à la fois contradictoires et généralement privées de tout ancrage dans le réel (histoire, sociologie, droit). La *blockchain* allait faire faire 20 milliards d'économie aux banques tout en nous permettant d'*uberiser Uber* en le privant de sa rente, de doter le Ghana ou le Honduras de cadastres pour y implanter les bases de la propriété tout en nous permettant de passer de l'économie de propriété à l'économie d'usage, d'échanger l'électricité produite sur nos toits avec des voisins qui en produisent et en consomment exactement sur les mêmes créneaux… Souvent en outre, la "*blockchain*" invoquée n'était rien de plus qu'un tableur Excel logé dans une Dropbox.

Coincées entre la menace des moustiques (les start-ups lancées par des *geek*s et qui profitent du côté tellement peu *user-friendly* des systèmes bancaires) et celle des mastodontes GAFAM repus de *data* collectées sur les réseaux mondiaux dont ils sont les maîtres, les vieilles institutions financières, protégées depuis des décennies par le mieux sécurisé des monopoles, handicapées par une pesante *legacy* informatique (des systèmes en COBOL parfois) virent dans leurs propres promesses l'espoir d'un espace de manœuvre. Au total, les économies promises ne venant pas, on finit par ne plus citer que les chiffres d'investissement.

Retour au transactionnel

La vraie nature du protocole *Bitcoin*, comme de ceux qui le copièrent ou qui, partant de ses intuitions géniales, le modifièrent avec d'autres paramètres exprimant d'autres préférences (*Ethereum*, notamment, plus "programmable", certes, mais au prix d'une moindre sécurité), c'est d'être des protocoles transactionnels. Non pas destinés à publier (comme TCP/IP) ou à s'écrire des messages (comme SMTP), mais à s'envoyer ces étranges "choses" que sont les jetons numériques.

Et donc, sur un protocole transactionnel, de nouvelles transactions apparurent. Non pas tant de substances illicites contre du *bitcoin* (ce qui avait été un cas d'usage non négligeable vers 2012) mais de "coin" contre "coin". Le sigle ICO, pour *Initial Coin Offering*, copiait assez clairement l'IPO (*Initial Public Offering*) pour que chacun comprenne bien qu'il s'agissait d'un appel public à l'épargne sauvage, hors de toute réglementation.

Les autorités s'émurent. L'absence de réglementation permettait évidemment toutes les malversations, et plus des trois-quarts de ces ICO furent douteuses. Mais quelle autorité de réglementation aurait apposé son "visa" sur des projets aussi prometteurs pour les initiés qu'incompréhensibles pour les béotiens qu'*Ethereum* (2014) ou *Tezos* (2016)? Ces deux projets ont pourtant, en quelque jours et sans grande formalité, sur un simple *white paper*, levé des centaines de millions d'euros, en *bitcoins* pour le premier, en *bitcoins* et en *ethers* pour le second. Les montants firent tourner la tête des escrocs, mais aussi des autorités et des politiques : la France se devait d'être la patrie des ICO. Durant toute l'année 2018, avec force auditions parlementaires et colloques à l'Autorité des Marchés Financiers, on accoucha d'un encadrement "à la française" des ICO, assez satisfaisant au demeurant, mais assez largement inutile puisque le taux de fiscalité sur les crypto-monnaies les chassent de France, pays dans lequel aucune banque,[6] en outre, n'entend faire la moindre concession sur son refus borné de la chose.

Au niveau mondial, le seul où s'appréhende la réalité de la cryptosphère, la concentration des plateformes de change se poursuit jusque pendant la crise du corona-virus, prouvant, certes en contradiction avec l'idéal initial de décentralisation, que les *blockchains* sont faites pour enregistrer des transactions sur des crypto-jetons, qu'on les appelle "*coins*", "*tokens*" ou comme on voudra.

Les générations de blockchains

On finit par distinguer plusieurs "générations" de *blockchains*. Ce classement est un peu artificiel, mais il est plus utile que le classement longtemps opéré entre *blockchains* publiques (sous-entendu : ouvertes à tout vent, ce qui est un contresens) et *blockchain* "privées" (sous-entendu: bien sécurisées, ce qui est contresens pire encore).

En gros, on dira que *Bitcoin* en 2009 et les premiers protocoles qui s'en inspirèrent (*Litecoin*, *Monero*) privilégiaient la sécurité absolue de la base de données et des transactions. Les *bitcoins* sont conservés dans un véritable coffre-fort numérique. Cela a son utilité, mais on devine qu'un coffre-fort n'est pas un instrument portable, maniable et simple d'usage pour les petits paiements. En 2014, un programmeur russo-canadien alors âgé de 19 ans, Vitalik Buterin, proposa une *blockchain* sensiblement différente, marquant une seconde génération. Parmi les ruptures proposées par *Ethereum*, on peut citer son langage de programmation plus accessible, l'existence d'adresses ne correspondant pas à tel ou tel détenteur mais à un programme traitant automatiquement les sommes reçues en fonction de son code (les *smart contracts*), enfin une gestion des actifs numériques détenus à chaque adresse assez similaire à celles des soldes de comptes bancaires, alors que *Bitcoin* traite les actifs en additionnant des restes "non dépensés" des transactions antérieures.[7]

---

[6] Et pas même les banques de l'État (Caisse des Dépôts et Consignations, Poste…), même lorsque le Parlement le leur demande, ce qui permet de mesurer certains rapports de force.

[7] Le débat théorique sur les avantages mutuels du système des "UTXO" de *Bitcoin* et du système par comptes d'*Ethereum* mérite un examen détaillé. Il est présenté aux pages 62 et suivantes du livre *Bitcoin et les protocoles à blockchain*, de Favier, Lécrivain & Takkal-Bataille, Liège, Mardaga Éditions, 2019.

Une troisième génération de *blockchain* regrouperait celles qui, pointant certaines limites des deux premières, et sans pour autant vouloir sacrifier la sécurité ou la programmabilité, cherchent à mettre en place des solutions pour une vraie mise à l'échelle et des mécanismes de gouvernance pour échapper au risque incessant de schisme (les *forks* de *Bitcoin*) ou de concentration du pouvoir. *Tezos*, *Cardano* ou *EOS* peuvent être citées ici.

Principes

S'il fut un temps permis de dire à peu près tout et n'importe quoi sur les *blockchains* ("*dans sa structure la plus simple, une* blockchain *n'est guère grand-chose de plus qu'une drôle de base de données*", selon Blythe Masters en 2015), il paraît important, en ce qui concerne les projets susceptibles d'intéresser la Défense, d'insister sur deux principes fondamentaux : la distribution des données, et celle du consensus.

Distribution des données

La distribution des données n'est pas en soi nouvelle ou révolutionnaire. En outre, il est facile de l'invoquer. Peu de fichiers informatiques n'ont jamais été copiés, que ce soit par la secrétaire de PME qui partait le soir avec la comptabilité sur une bande de secours ou par le cadre qui emporte un back-up sur une clé USB. Faible distribution, actualisation épisodique, le soir ou le week-end, et procédé douteux que ce soit pour conforter la sécurité (c'est mieux que rien) ou pour la compromettre (vol de données, chantages, fuites). Même les données conservées dans des *silos* informatiques sécurisés sont copiés dans un second silo. Il ne s'agit pas de cela.

La distribution au sens où on l'entend dans l'industrie de la *blockchain* implique que les copies soient automatiquement répliquées en temps réel sur le réseau, et que ce réseau, en l'absence de tout serveur central et de toute hiérarchie entre les serveurs, ait la forme d'un filet de mailles, non d'une étoile. Dans l'idéal, les éléments de ce réseau ne doivent même pas se connaître entre eux. Une base de données, même "distribuée" dans les 2000 agences du plus grand réseau bancaire de France, serait de taille respectable, mais resterait sujette au risque de subordination hiérarchique ou de collusion, par exemple pour effacer une erreur de la banque.

Une distribution hétérogène, sinon aléatoire, des éléments du réseau est donc largement aussi importante que le nombre de ces éléments. Il y a des milliers de "nœuds" de grandes *blockchains* ouvertes comme *Bitcoin*, *Ethereum* ou *Tezos*, mais 101 validateurs pour *Ark* ou 21 pour *EOS*. Enfin, on peut citer les 13 serveurs racine du DNS, c'est-à-dire le service informatique distribué utilisé pour traduire les noms de domaine Internet en adresses IP ou autres enregistrements.

Distribution du consensus

La distribution du consensus doit être considérée séparément. Un réseau peut être largement distribué en ce qui concerne les nœuds "passifs" (les livres de compte répliqués) mais leur grand nombre n'apporte pas une garantie robuste si la validation des écritures est le fait de quelques-uns seulement. En juin 2016, la rapidité avec laquelle a été prise la décision, pourtant très lourde de conséquences, de créer un nouvel *Ethereum* ne prenant

pas en compte une transaction viciée support d'un "*hack*"[8] a suscité le soupçon que la concentration de la décision n'était guère différente de ce qu'elle aurait été dans une banque ou une administration centralisée.

Au-delà des grandes déclarations qui font de la *blockchain* une chose infalsifiable par nature, il faut donc au contraire regarder l'ingénierie humaine : la façon dont le consensus sur la validation est concrètement mis en œuvre, par qui, et avec quels risques de fraude, collusion, alignement des intérêts, subordination, ou capitulation devant un chantage, etc. Il ne faut pas oublier qu'au-dessus du consensus algorithmique, il demeure toujours (même peu visible) un consensus social, c'est à dire humain.

Usages connus et potentiels

Une rapide navigation sur Internet donne beaucoup trop de cas d'usage, dont certains sont presque fantaisistes, soit parce que la mise en œuvre d'une *blockchain* n'y apporte rigoureusement rien, soit parce que l'usage en est futile. Inscrire sa déclaration d'amour sur une *blockchain* ne vaut ni plus ni moins qu'un cœur gravé sur un tronc en forêt ou un cadenas sur le Pont des Arts. Qu'en est-il des usages réellement prometteurs ?

Règlements et billetterie

Si la monnaie est incontestablement le cas d'usage natif de la *blockchain*, c'est sous la forme de monnaie *sui generis*. Cela ne crée pas seulement des problèmes politiques aux États (doivent-ils tolérer l'existence d'une monnaie non régalienne ?) mais aussi des problèmes technologiques (peuvent-ils en faire autant ?). Or, si jouer au Monopoly avec des billets légaux ne poserait aucun problème (sauf légal !), créer des jetons numériques en euros est plus compliqué. Au fond, on tend laborieusement à réintroduire le problème dont Satoshi Nakamoto s'était abstrait !

Chacun cherche à émettre des *stable coins*, c'est à dire des vrais jetons transférables sur une *blockchain* et qui, par convention, par contrat, ou par la confiance qu'inspirerait une réserve à 1 pour 1 constituée en monnaie légale, vaudraient leur valeur faciale en monnaie légale.

Le projet *Libra* de Facebook tourne autour de cette notion. Celui de la banque américaine J.P. Morgan aussi. Des centaines de jetons mettent aussi en œuvre cette idée bancale en réintroduisant fatalement une dimension fiduciaire pour justifier le grand retour des "réserves fractionnaires", à l'image de l'USDT de *Tether* (le plus connu des *stable coins*) qui n'a pas tenu cinq ans un engagement de réserves à 1 pour 1 que les Banques centrales historiques avaient mis des décennies à assouplir.[9] L'USDT, officiellement couvert aujourd'hui à 88% par du dollar, cote toujours autour de 1$, compte tenu des services qu'il rend dans la cryptosphère. Douteux miracle.

À terme, fatalement, existeront des monnaies cryptographiques fiduciaires, émises par des autorités politiques habilitées, sur des *blockchains* offrant toutes garanties de

[8] Pour un historique de cet événement, lire le texte de Benoît Huguet, à l'adresse : https://bitconseil.fr/thedao-hack-etat-lieux-perspectives/.

[9] Sur la gestion très "créative" de la Banque de France au 19e siècle, une fascinante étude historique est en ligne ici : https://www.persee.fr/doc/ahess_0395-2649_1996_num_51_4_410891.

sécurité, et valant une unité de compte légale sans plus de "réserve" qu'il n'y en a pour un billet de banque centrale, juste par geste souverain (on les désigne par un mot latin comme des monnaies "fiat"). Les obstacles sont en fait politiques. Les îles Marshall, dans leur coin perdu, ont déjà réalisé la chose de façon très intéressante et sur une *blockchain* peu connue du grand public (*Algorand*, développée dans l'orbite du MIT) et avec l'aide de la start-up israélienne Neema comme intégrateur.[10]

En regard, la plupart des Banques centrales ont des projets prudents, toujours plus ou moins inspirés de l'exemple de l'*e-krona* suédoise.[11] La Banque de France a mené des "expérimentations" et lancé un appel à projets concernant la création d'une "monnaie digitale de banque centrale", mais avec l'objectif restreint de tester une monnaie inter-bancaire qui puisse servir de prototype en vue d'un éventuel futur "euro digital".

Le rapport rédigé par Jean-Pierre Landau en juillet 2018 avait évoqué la numérisation d'une partie de la billetterie des Jeux olympiques de 2024.[12] Une telle initiative, sans empiéter sur le pré carré jalousement gardé des monnaies légales, serait très opportune.

Un cas de figure particulier est représenté par les "monnaies de crise" que l'on pourrait qualifier de "monnaies de siège 2.0". La Banque de France a ainsi présenté en janvier 2020 à l'Institut d'Émission des DOM un dispositif pour un "cas Saint-Martin"[13] permettant, après une catastrophe naturelle, la mise en place d'une forme d'identité numérique, d'une solution de traçabilité des lots de secours, et d'une monnaie numérique dédiée. Le tout codé sur la *blockchain Tezos*, issue de la recherche scientifique française dont il va être question plus loin.

Il est clair que dans des scenarios extrêmes, une monnaie de secours déployée en quelques heures sur des portefeuilles numériques téléchargeables par téléphone pourrait rendre de signalés service aux Armées, dans le cadre d'opérations de distribution de secours (médicaments, etc.) à des populations traumatisées par une catastrophe nucléaire, climatique ou sanitaire, en évitant aussi le marché noir inhérent aux distributions non contrôlées.

Une telle monnaie aurait aussi sa place dans le cadre de possibles conflits de haute intensité, en permettant le déploiement d'une solution de secours immédiatement exploitable sur le théâtre sinistré, notamment dans le cas d'un déploiement en primo-intervenant des forces armées en territoire hostile. Si une occupation militaire, pour reprendre les mots du Maréchal Lyautey "*consiste moins en opérations militaires qu'en une organisation qui marche*", la gestion de nouvelles zones à stabiliser justifie la conquête de nouvelles ressources technologiques et l'adoption par les forces armées d'innovations, notamment en matière de déploiement opérationnel et de traçabilité des flux.

---

[10] *Cf.* https://www.algorand.com/resources/news/marshall-islands-to-power-worlds-first-national-digital.

[11] Voir : https://www.riksbank.se/en-gb/payments--cash/e-krona/ avec des notes techniques en lien.

[12] https://www.mindfintech.fr/files/documents/Etudes/Landau_rapport_cryptomonnaies_2018.pdf.

[13] L'ouragan *Irma* qui frappa cette île le 6 septembre 2017 a provoqué de nombreuses réflexions, y compris sur la résilience réelle des systèmes politiques et administratifs. Lire, entre démenti et aveu, "Irma : attention aux rumeurs sur la situation à Saint-Martin" (in *Le Monde*, 9 septembre 2017) : https://www.lemonde.fr/les-decodeurs/article/2017/09/11/irma-attention-aux-rumeurs-sur-la-situation-a-saint-martin_5184022_4355770.html.

Notarisation et traçabilité (du luxe/ de l'Aérospatiale, ou de la Défense)

Dès qu'il a été affirmé que la *blockchain* permettait un "traçage", elle a suscité l'intérêt d'un secteur très particulier, celui de l'industrie du luxe. La grande distribution a emboîté le pas, garantissant la traçabilité du miel français, des œufs bio ou des poulets de plein air. Il n'est pourtant pas évident qu'une *blockchain* apporte une réelle plus-value par rapport à un simple procédé de signatures à clés asymétriques. La distribution des rôles de validateurs reste souvent le point critiquable des projets. En outre demeure le problème d'un réel "lien" entre les jetons cryptographiques qui font l'objet des transactions sécurisées sur la *blockchain* et les objets physiques (vins, maroquinerie…) qu'ils sont censés représenter. Le traçage des montres de luxe mis au point par la start-up française Woleet pour le compte de Kering[14] inscrit en réalité le *hash* du certificat d'authenticité que l'acheteur reçoit aussi par fichier PDF après son achat. C'est sans doute mieux qu'un filigrane sur un document, mais cela ne saurait suffire pour des usages stratégiques, ou pour tracer des stocks importants de munitions.

Les secteurs hautement stratégiques que sont la Défense et l'Aérospatiale pourraient, avec des projets plus ambitieux (c'est un point à souligner) bénéficier des apports de la technologie des *blockchains*, au premier rang desquels la traçabilité et la confidentialité. Ainsi, dans l'ombre portée du désastre d'Ariane 5 en 1996, il était apparu essentiel de s'assurer de la bonne maîtrise de la chaîne logistique et de la possibilité d'en vérifier le bon fonctionnement *a priori*. *Tezos*, unique protocole européen dont les langages de programmation supportent la "vérification formelle", ouvre à la possibilité d'une vérification mathématique du bon fonctionnement des programmes déployés en amont de leur mise en production.

Le vote

Geste sacré de la liturgie démocratique, le vote s'apparente pourtant par bien des aspects à une transaction : chaque électeur dispose d'un "droit" à envoyer **1** à l'un des candidats et **0** aux autres. Les problèmes d'identification de l'électeur, d'anonymat de son vote et de dépouillement du scrutin sont tous de ceux qu'une *blockchain* peut résoudre.

Encore faut-il ne pas se bercer de mots. Le vote sur la *blockchain* prévu en Virginie Occidentale a été annoncé un peu vite (l'expérience ne concernait que 2 comtés pour les seuls électeurs absents ou handicapés) et elle a été pour l'instant partiellement abandonnée…en raison de failles de sécurité.[15] L'expérience locale menée à Zoug n'est pas non plus exempte de critiques,[16] mais les fiascos en matière de vote "non physique" ne sont pas réservés aux seules expériences sur des *blockchains*, comme le cas de l'*e-voting* genevois le rappelle.[17]

---

[14] Une présentation de l'opération existe à l'adresse : https://www.capital.fr/entreprises-marches/comment-kering-utilise-le-bitcoin-pour-certifier-ses-montres-de-luxe-1359862.

[15] *Cf.* https://www.blockchainmagazine.net/west-virginia-dumps-blockchain-based-voting-app-voatz-due-to-security-issues/.

[16] Voir : https://www.letemps.ch/suisse/zoug-teste-vote-electronique-blockchain.

[17] Sur cette expérience : *cf.* https://www.swissinfo.ch/fre/point-de-vue_les-bases-d-un-vote-électronique-sécurisé-et-démocratique/44608066.

La pandémie du Covid-19 a tout de même souligné, aussi, la faiblesse de la "logistique démocratique". La plupart des pays européens ont reporté *sine die* les diverses consultations en cours ou prévues. Il faut tout de même rappeler que l'Article 7 de notre Constitution ne permettrait pas semblable bricolage en ce qui concerne un scrutin présidentiel. Et *de facto*, les ressources constitutionnelles du référendum ou de la dissolution de l'Assemblée nationale peuvent être mises hors-jeu par un confinement. Le sujet d'un vote "en ligne" n'est donc pas forcément un fantasme de *geek*, et pourrait utilement être exploré au-delà d'expériences locales avant que la chose ne tourne à la crise politique grave.

Transactions diverses, dans le redoutable "Internet des Objets"

De nombreux cas existent où des machines entrent en transaction entre elles. Comme elles n'ont pas de personnalité juridique mais une puissance de calcul, la *blockchain* apparaît idéale pour elles. Pour l'instant, même pour faire des transactions avec des êtres humains, les machines doivent passer par des tiers. Toute l'information n'est pas dans la machine ou sur la carte à puce, et à un moment ou à un autre une banque est interrogée, avec ce que cela implique en termes de délais et de frais de transaction.

Ainsi, dans les transports urbains, les machines font appel à un processeur de paiement pour accepter les cartes bleues, parce que des paiements préacceptés exposeraient à un risque de fraude. Les sociétés fournissent donc des tickets ou des cartes rechargeables à l'unité (*Oyster* à Londres) ou au forfait (*Navigo* à Paris), ce qui leur permet au moment du passage au portique d'éviter de faire de longues et coûteuses requêtes bancaires. Il n'y aurait rien de tout cela avec une "vraie" monnaie cryptographique. Dans le métro, sur les autoroutes, ou à l'entrée des musées, des portiques détenteurs d'un portefeuille cryptographique qu'ils rempliraient et décaisseraient automatiquement, ou qui scruteraient eux-mêmes la *blockchain* pour savoir si le paiement est passé, offriraient une solution efficiente et peu onéreuse, avec en outre une preuve de paiement en cas de problème.

Il faut cependant être conscient des failles de sécurité qui affectent déjà les objets connectés. De telles transactions, en matière de santé, de transport ou de défense nécessiteraient une *blockchain* dont les contrats auto-exécutables seraient autrement résistants aux *hacks* que ceux que l'on voit aujourd'hui codés en employant des langages, certes très faciles mais non statiquement typés, non fonctionnels, sans sémantique formelle.

Les militaires en pointe dans ce domaine

Plusieurs signes, plus ou moins médiatisés, permettent d'affirmer que les militaires ont abordé la technologie des *blockchains* pragmatiquement, sans les pudeurs ou les rancœurs dont on faisait preuve dans d'autres milieux.

La Gendarmerie

Gendarmes comme voleurs?

Que le *bitcoin* soit ou non une monnaie de délinquants (qu'il l'ait été à ses débuts fait peu de doute[18]) a pu mener très vite des politiques à en demander l'interdiction. Mais,

[18] La chose est abordée assez en détail *in* Jacques Favier & Adli Takkal-Bataille, *Bitcoin, la monnaie acéphale*, *op.cit.*, pp.174-177.

dans l'éternel jeu du gendarme et du voleur, les gendarmes se sont très vite saisis de cet "instrument de travail".[19]

En France, la Gendarmerie a organisé sa chaîne cybercriminalité en l'appuyant sur un réseau de proximité au niveau local (référents Cyber), sur des spécialistes au niveau départemental (Cyber N'Tech) et des experts au niveau national (PJGN) réunissant les compétences de pointe du C3N et du département informatique électronique de l'IRCGN.

Ce centre de lutte contre les criminalités numériques (C3N) travaille pour l'essentiel d'initiative. Ses enquêteurs disposent d'une compétence nationale et sont formés à l'enquête sous pseudonyme sur Internet. Ils utilisent des logiciels élaborés leur permettant d'investiguer sur l'ensemble des vecteurs, que ce soit le web classique, les réseaux sociaux, le *dark web*, les jeux vidéo connectés, et naturellement… les transactions en *bitcoins*. Ils le font grâce à une veille permanente. Les champs infractionnels prioritaires que poursuit le C3N sont les ventes de stupéfiants ou de faux documents, les atteintes aux systèmes de traitements automatisés de données (p.ex.: *ransomware*) et la pédopornographie, mais aussi des matières "militaires" comme l'apologie du terrorisme et ses réseaux, ou les trafics d'armes.

En France, où le média phare de la communauté "Bitcoin" avait en 2013 salué sans équivoque,[20] après l'arrestation du créateur de la *Silk Road* et la fermeture de ce site, des contacts responsables, et pour tout dire cordiaux, se sont noués entre des gendarmes suffisamment formés pour faire la part des choses et échanger sur la base de respect mutuel que permet une égale connaissance d'un sujet très technique et des membres de l'association "Le Cercle du Coin". Le capitaine Édouard Klein du C3N est ainsi intervenu (à titre privé) lors d'un colloque pluridisciplinaire organisé par cette association en mai 2017 à l'École Normale Supérieure. L'année suivante, lors d'un *meet-up* du même Cercle organisé à Bordeaux, c'est Stéphane Tonelli, chef de groupe cybercrime et enquêteur spécialisé dans les TIC qui intervenait pour répondre à la question "Bitcoin est-il le cauchemar du gendarme ? Ce qu'apprend l'expérience".

En décembre 2018, La *Revue de la Gendarmerie nationale* consacrait 38 pages de son n°263 aux *blockchains* et à *Bitcoin* en particulier, à travers quatre dossiers:

- *Blockchain* : Sécurité et confidentialité (Gilles Hilary, chercheur associé au CREOGN)
- La *blockchain* est-elle un tournant stratégique ? (Olivier Kempf)
- Crypto-tracking, les nouveaux outils d'enquête pour les forces de l'ordre (Adel Jomni)
- L'État ne sait pas assiéger Byzance ? (Capitaine Édouard Klein, C3N).

Parmi les idées fortes on trouvait qu'il est illusoire de légiférer contre la réalité ("interdire le bitcoin", "censurer la *blockchain*", etc.); que les interactions entre le monde réel et la *blockchain* sont assez nombreuses pour que les forces de l'ordre puissent y

---

[19] Maître Michelle Abraham a écrit sur ce thème : https://bitcoin.fr/les-gendarmes-les-voleurs-et-bitcoin-2-2/.
[20] *Cf.* https://bitcoin.fr/fermeture-de-silk-road-enfin/.

travailler utilement, et qu'ainsi le vrai défi pour la protection du citoyen réside dans la compréhension par le grand public des concepts et techniques et dans l'accompagnement de l'innovation par les gendarmes chercheurs et ingénieurs dont le niveau en France ne fait pas rougir. Le C3N allait d'ailleurs le prouver bientôt en s'illustrant par une démarche novatrice audacieuse.

Le premier smart contract *créé par une institution gouvernementale*

Le 6 septembre 2019 eut lieu la première utilisation opérationnelle au monde d'un *smart contract* par une entité gouvernementale. Le C3N, l'unité nationale de lutte contre la cybercriminalité de la Gendarmerie nationale, devait notariser les justifications de dépenses effectuées dans le cadre d'une subvention fournie par Europol et elle a choisi de le faire grâce à un *smart contract* déployé en production sur la *blockchain* publique *Tezos*.[21]

Grâce à cela, en un clic, le gendarme peut diffuser sur Internet la trace infalsifiable du document comptable qu'il vient d'éditer. Dans les secondes qui suivent, des milliers d'ordinateurs à travers le monde exécutent une même suite d'opérations élémentaires, vérifiant l'identité de l'auteur de la trace et validant la trace elle-même. Ces ordinateurs comparent entre eux le résultat obtenu et en inscrivent la trace dans un registre dont ils gardent chacun une copie, protégée de toute tentative d'altérations malveillantes ou d'erreurs des autres membres du réseau.

Des mois plus tard, alors qu'il rend compte à l'organisme de contrôle de l'utilisation des fonds qui lui ont été confiés, ce même gendarme pointe vers la trace qui dort, inaltérable, dans le registre mille fois vérifié et dupliqué. Cette trace prouve indubitablement que la comptabilité qu'il présente est bien celle qu'il avait établie à l'époque. Toute comptabilité créative visant à masquer *a posteriori* une malversation ou une erreur lui est devenue impossible, il ne peut que présenter une comptabilité conforme à la trace.

Le coût de cette traçabilité infalsifiable et transparente? Moins de trois dixièmes de centimes par enregistrement. Cette *preuve de concept* ouvre la voie à un changement de paradigme comptable, à la fluidification de la réponse logistique aux besoins opérationnels et à d'autres applications de la *blockchain* (intégrité de la preuve numérique, chaîne de responsabilité, etc.) aux enquêtes cyber.

Cette révolution comptable est aussi un soulagement opérationnel par rapport au modèle actuel de l'autorisation préalable. Selon ce modèle, en effet, pour déclencher une dépense, un gendarme doit formuler sa demande à travers un logiciel obsolète. Il doit ensuite faire valider sa demande, via ce logiciel obsolète, par toute la chaîne hiérarchique jusqu'à atteindre un militaire autorisé à autoriser sa demande: en pratique, un général ou un colonel, même pour des montants minimes. Le service idoine va ensuite s'assurer que le fournisseur est référencé et gérer la séquence habituelle : devis, bon de commande, livraison, facture, paiement. Du moins en théorie. En pratique, le gendarme va devoir relancer plusieurs fois le service idoine et faire une partie du travail à sa place (typiquement transmettre le devis et les informations nécessaires au référencement et gérer

[21] *Cf.* https://tzscan.io/KT1Gbu1Gm2U47Pmq9VP7ZMy3ZLKecodquAh4?default=code.

les relations avec les fournisseurs, qui peuvent devenir houleuses en cas de retards de paiement, hélas trop fréquents). Lorsque les montants dépassent un certain seuil, il faut alors faire intervenir le mécanisme des marchés publics, et tout espoir d'accomplir la moindre avancée opérationnelle est perdu pendant plusieurs mois.

Dans le nouveau modèle, qui fonctionne avec un contrôle *a posteriori*, on attribue aux gendarmes concernés selon leur grade et leur fonction les moyens d'accomplir leur mission, ou à défaut une part des moyens disponibles. Cette attribution a lieu sous la forme d'un moyen de paiement personnel, sécurisé et bloqué: les dépenses sont tracées, il est dès lors impossible de dépenser les sous du voisin, et impossible de dépasser le plafond de dépenses autorisées. À chaque événement de paiement, le gendarme rajoute une ligne au tableau des comptes et enregistre le ou les documents justifiant la dépense. Le logiciel calcule alors une trace infalsifiable de ces modifications. Si ne fût-ce qu'un *bit* changeait, toute la trace serait modifiée. Lors du téléversement des modifications, cette trace est mise à jour dans le registre public et partagé. Toute l'opération, du choix du prestataire jusqu'à la diffusion de la trace, n'a pris que quelques minutes et n'a coûté que quelques centimes en frais de gestion et d'infrastructure. Bref, vingt lignes de code remplacent, de manière avantageuse, trente bureaucrates.

Il est alors possible de contrôler les dépenses *a posteriori*, tout comme l'est le contrôle systématique encore en vigueur. Néanmoins, il n'est probablement pas souhaitable. Le contrôle d'un échantillon réduit mais représentatif est suffisant à la maîtrise des risques et au contrôle de la légitimité et de la conformité des dépenses. Grâce à la subvention d'Europol, la dépense bloquée depuis quatre mois dans le processus normal d'approbation préalable est effectuée en quelques minutes, et sa justification inscrite dans le registre infalsifiable.

Cette innovation a pu avoir lieu au C3N grâce à la souplesse d'action dont jouit son département technique, où sont affectés les sous-officiers les plus "pointus" techniquement ainsi que des officiers commissionnés issus du monde académique et du secteur privé. S'ils ne disposent que de peu de moyens, ils ont au moins la liberté d'expérimenter au profit des enquêteurs qu'ils côtoient et qu'ils épaulent au quotidien.

Néanmoins, cette capacité d'adaptation des solutions technologiques aux besoins de l'arme est mise à mal par la vision gestionnaire et bureaucratique de l'état-major. Sans efforts significatifs et immédiats visant à garantir cette liberté d'action et à l'appuyer par un effort budgétaire conséquent, les innovations comme celle présentée dans cet article ne verront aucune suite et cesseront de se produire.

Transparence, secret, confiance

La transparence est la pierre angulaire de la démocratie. Le peuple doit pouvoir contrôler ou faire contrôler par ses représentants la dépense publique. Pour autant, le secret de l'enquête ne saurait être violé. Que ce soit pour protéger l'enquête elle-même, ou la vie privée des citoyens qui en sont l'objet. Les activités opérationnelles des forces de sécurité ont donc besoin d'être protégées par le secret.

Comment conjuguer le besoin du secret avec la nécessité de la transparence? Le *smart contract* mis en place par le C3N ne diffuse que les traces de la comptabilité. Si les

traces sont cryptographiquement liées au contenu de la compatibilité, au point même que changer un seul chiffre change toute la trace, cela ne signifie pas qu'il soit possible de remonter de la trace vers le contenu, bien au contraire.

Par exemple, à l'heure d'écriture de ces lignes, la dernière trace diffusée sur le *smart contract* était *7596a56e8e4bf7eae481b3f1e6f000d1ff0bf258*. Impossible à quiconque de remonter sur les fichiers ayant généré cette trace. En revanche, le public peut exiger, en temps utile, de voir les fichiers (et leur historique intégral) correspondant à la trace ainsi laissée : *7596a56e8e4bf7eae481b3f1e6f000d1ff0bf258*. Cette trace est la seule chose qui soit publique, elle ne met donc pas en danger les activités opérationnelles du C3N, mais étant publique elle oblige le C3N à une rigueur parfaite dans la tenue des comptes, et à préparer la justification des dépenses, comme on est en droit de l'attendre de toute unité dépensant de l'argent public. La permanence et l'intégrité des registres comptables habituels sont garanties par la fiabilité de l'agent (souvent assermenté) qui les renseigne et les manipule.

Grâce à ce nouveau système, la confiance dans le registre ne dépend pas de comportements individuels par nature susceptibles d'erreurs (ou pire). Elle repose dans le fait que plusieurs milliers de machines, détenues par des agents n'ayant aucune raison de comploter ensemble pour falsifier le registre, dans un réseau ouvert à tous, vont tous faire fonctionner le *smart contract*, et ne vont entériner la transaction que lorsque le consensus sur la bonne exécution du code est atteint. Le tout pour moins d'un centime d'euro ! C'est une nouvelle source d'erreur et de coût qu'on élimine.

Le *smart contract* a été codé de manière à maintenir une liste des personnes autorisées à diffuser une nouvelle trace ou à changer la liste des personnes autorisées. Il vérifie également que la personne qui diffuse une nouvelle trace connaît la trace actuelle. Toute transaction ne répondant pas à ces deux critères sera rejetée par le code.

Le code du *smart contract* est extrêmement simple, et donc facile à vérifier.[22] Comme son exécution conforme est garantie par la multiplicité des acteurs du registre, le public peut avoir toute confiance dans le système et savoir que la trace stockée dans le registre est bien la dernière trace à jour diffusée par les enquêteurs du C3N.

Pour les petites dépenses, la *blockchain* ne présente donc aucun désavantage par rapport à la méthode actuelle et l'application du type de procédure qui vient d'être décrite pourrait être immédiate et généralisée. Il n'est peut-être pas souhaitable de détrôner immédiatement les marchés publics pour les grosses dépenses, bien que là aussi des *smart contracts* pourraient aider à fluidifier les processus.

L'expérience a eu le mérite de roder les équipes à un protocole particulier, d'ailleurs avec le soutien de Nomadic Labs, société filiale à 100% de la Fondation Tezos.

---

[22] Le code du *smart contract* et des scripts associés est disponible, pour les lecteurs à qui le détail technique ne fait pas peur, à l'adresse : https://gitlab.com/edouardklein/notarizedaccountability. L'explication de l'implémentation est la suivante : les enquêteurs poussent les fichiers de comptabilité dans un *repo git*, où le *hook pre-receive* se charge d'effectuer une transaction sur le *smart contract*, publiant ainsi le *hash* du dernier *commit* reçu. Un échec de la transaction entraîne un rejet du *commit*.

Les raisons du choix d'un protocole particulier

Tezos a été choisi par le C3N pour des raisons techniques. La première, fondamentale, est qu'il faut que la *blockchain* soit en mesure d'interpréter un langage suffisamment complexe pour permettre l'écriture de *smart contracts*. Cela élimine par exemple *Bitcoin*, dont le langage d'écriture des transactions ne permet que des opérations trop simples pour y coder une logique complexe. Il n'est pas "*Turing-complet*".

Son absence de complexité a des avantages certains, puisqu'elle permet d'avoir des garanties *a priori* sur toutes les transactions, comme par exemple de donner la mémoire maximum qu'il faut pour les vérifier. Mais dès que l'on saute le pas de la *Turing Completude*, toutes ces garanties s'envolent et il devient impossible de dire, pour toutes les transactions en général, si l'on pourra les exécuter sous certaines contraintes (de temps, de mémoire, etc.). C'est le théorème de Rice.

Le deuxième candidat logique était donc *Ethereum*, dont le langage de transaction (Solidity) est Turing-complet. Malheureusement, le langage a été jugé mal conçu[23] parce qu'il est trop facile d'introduire des bugs dans les *smart contracts*.

Tezos corrige ces problèmes avec un langage de "bas niveau", le Michelson, qui est suffisamment complexe pour écrire des *smart contracts*, mais suffisamment simple et rigoureux pour qu'un *smart contract* puisse être analysé semi-automatiquement par une machine. Cette analyse semi-automatique (le système de types) élimine toute une classe de bugs qui pourrait se trouver dans le même contrat écrit en Solidity.

De plus, il est possible d'étudier mathématiquement le code d'un contrat particulier et de retrouver pour ce contrat précis les garanties que l'on a pour tous les contrats avec un langage non *Turing-complet*. Cette preuve mathématique se fait à l'aide d'un assistant de preuve numérique, ce qui élimine beaucoup d'erreurs humaines.[24]

Autres exemples en France

Les Armées ont perçu assez vite, sinon tout le potentiel de la *blockchain* (encore largement expérimentale en ses diverses "*proofs of concept*"), du moins sa fonction de remise en cause d'idées acquises. La *blockchain* était donc dans les radars de nombreuses publications.[25] C'est ainsi qu'en septembre 2018 un article présentait la technologie et en recensait quelques applications possibles[26] (messagerie sécurisée, gestion des identités, logistique et suivi du matériel sensible), et qu'en octobre 2019 un autre article traçant une

---

[23] *Cf.* https://news.ycombinator.com/item?id=14691212.

[24] Si *Tezos* et le langage Michelson se prêtent si bien à cette mécanique rigoureuse qui permet de contourner le théorème de Rice, c'est parce que le code a été conçu par des ingénieurs et chercheurs de très haut niveau. Chercheurs dont il n'est pas indécent de noter qu'ils sont, pour une bonne partie d'entre eux, issus de la recherche française (notamment de l'INRIA et de l'École Normale Supérieure), à la pointe dans ce domaine depuis plusieurs décennies avec des projets comme Coq et OCaml. Est-il étroitement nationaliste de saluer l'inscription de cette *blockchain* de troisième génération dans un écosystème d'institutions et de chercheurs français?

[25] Par exemple, *L'Observatoire du monde cybernétique*, animé pour le compte de la Direction générale des relations internationales et de la stratégie (DGRIS) du ministère des Armées par la Compagnie européenne d'intelligence stratégique (CEIS).

[26] Voir : https://omc.ceis.eu/la-blockchain-et-ses-usages-militaires/.

Géopolitique de la blockchain[27] recensait quelques menaces (terrorisme, pressions diplomatiques), mais aussi quelques opportunités.

Les Armées et services en opérations extérieures

L'affrontement des volontés, typique des conflits armés, ainsi que l'incertitude qui en résulte, ont fait de la capacité à penser et à transmettre l'information le centre de gravité de nos forces. C'est ainsi que depuis trente ans les évolutions les plus notables portent sur les technologies d'information et de communication.

Qu'il s'agisse d'une escadrille de chasse, d'un groupe aéronaval ou d'un groupement tactique interarmes, tous s'appuient sur un même type d'architecture radio : qu'on l'appelle "maître-esclave" ou "en étoile", son principe est celui d'une station directrice chargée d'animer le réseau constitué avec ses stations secondaires. Ce type de réseau est fortement centralisé, et donc, vulnérable.

Une *blockchain*, en apportant une organisation décentralisée, pourrait améliorer la résilience des structures de *command and control* (fonction englobant l'ensemble des moyens et capacités mise en œuvre pour commander une unité) qui sont aujourd'hui déployées via ces réseaux centralisés. La technologie n'étant pas encore consolidée, il s'agit surtout ici – sans tomber dans le travers de l'effet de mode – d'envisager les cas d'usages possibles de façon réaliste et utile, et ils sont nombreux !

En effet, une arborescence réellement maillée serait un atout pour toute formation militaire en phase d'approche ou d'abordage de son ennemi. Considérant que dans un contexte dont on dit qu'il verra le retour de la puissance et de la haute intensité, les attaques sur nos réseaux radios et informatiques seront nombreuses, la centralisation pourrait être un handicap. Les forces loyalistes ukrainiennes en ont fait l'expérience en 2017 lorsqu'elles ont vu un de leurs postes de commandement neutralisé par une action combinée de la guerre électronique (unités chargées de la maîtrise du spectre électromagnétique : intrusion, détection, brouillage des émissions adverses) et de l'artillerie russes. Les capacités subordonnées à ce poste de commandement se sont alors vraisemblablement retrouvées comme un poulet sans tête. Les Russes l'ont compris: nos organisations sont très vulnérables en leur centre, les stations directrices étant de réels goulets d'étranglement. Elles ont en outre la fâcheuse caractéristique d'émettre beaucoup plus fort que les autres stations pour les atteindre toutes, facilitant le travail du renseignement adverse.

Ce fait est révélateur d'un problème militaire en passe de devenir critique. La décentralisation permise par la technologie des *blockchains* pourrait être un moyen d'y remédier. Si les forces armées adoptaient des protocoles de communication nativement chiffrés dont les messages sont transmis de station en station en suivant le chemin le plus direct, la perte d'un "nœud" du réseau, même central, n'aurait pas d'incidence sur la transmissibilité. La résilience d'une troupe ainsi équipée s'en trouverait nettement améliorée.

---

[27] *Cf.* https://omc.ceis.eu/geopolitique-de-la-blockchain/.

Et l'intérêt de ce type de fonctionnement est universel : des équipes de Forces spéciales en infiltration jusqu'à la patrouille de bombardiers en mission de raid en passant par des frégates en combat de surface, c'est l'ensemble des forces armées qui s'en trouveraient renforcées.[28]

Au-delà des fonctions qui délivrent le feu, les fonctions support gagneraient également à envisager ce fonctionnement décentralisé. La logistique de transport, faisant le choix d'une numérisation intégrale en s'appuyant sur les technologies RFID et *blockchain* pourrait enfin obtenir une vision exhaustive et en temps réel de l'intégralité de ses flux. Sa politique de maintenance, surtout sur les théâtres d'opérations, en serait grandement améliorée.[29]

Aux gains en efficacité s'ajoutent des perspectives d'économie : une enquête réalisée par un cabinet d'IBM évalue celles-ci à 20%, surtout en raison des procédures administratives simplifiées. Un portage des données de logistique sur une telle solution pourrait également permettre des rapports plus forts et plus clairs avec les entreprises civiles. En effet, une infrastructure semi-ouverte permettrait aux contractants civils de s'interfacer plus facilement, et même d'enregistrer dans la *blockchain* des contrats intelligents, les fameux *smart contracts*, des contrats dont les conditions de réalisation sont codées et exécutées automatiquement lorsque les conditions définies sont remplies.

Pour la fonction connaissance-anticipation, autrement dit pour le renseignement, la question de la bascule sur une *blockchain* est plus difficile. Comme pour les données "opérationnelles", le niveau de classification élevé nécessitera une ingénierie informatique particulière. En revanche, la différence porte sur l'importance centrale des bases de données pour les métiers du renseignement. En effet, dans ce métier, l'incident observé prend tout son sens après comparaison avec la photo globale, soit la donnée stockée en base. Or, ces bases de données possèdent un très haut niveau de confidentialité : il s'agit vraiment des joyaux de la couronne. Aussi, la politique actuelle consiste à dégrader la base de données au fur et à mesure qu'on s'approche de la zone d'insécurité, pour limiter le risque de compromission en cas de perte de la base. Il en ressort que la distribution décentralisée des bases de données "renseignement" ne pourra se faire qu'au prix d'une robustesse, au plan logique, équivalente à celle que l'on a au plan organisationnel. Cependant, des politiques militaires récentes dans la sécurité des systèmes d'information laissent entrevoir des possibilités.

Le sens de l'histoire semble indiquer aux forces armées la nécessité de repenser leurs modes d'échange avec davantage de décentralisation. L'avènement progressif du combat collaboratif y encourage : le programme SCORPION dotera l'armée de Terre de capacités de combat améliorées grâce à une communication automatisée entre hommes ainsi qu'entre hommes et machines. Néanmoins, l'adoption franche de cette technologie pourrait advenir plus facilement en métropole.

---

[28] Cette ambition d'un réseau robuste est prise en compte par les modes de transmission de nouvelle génération proposant nativement des services de relais dans les postes radios, notamment CONTACT. Une architecture à mi-chemin entre la centralisation néfaste et une totale décentralisation.

[29] C'est ce cas d'usage que les Armées ont décidé d'expérimenter, la SIMMT (structure intégrée du maintien en condition opérationnelle des matériels terrestres) étant actuellement en phase d'évaluation d'un projet d'envergure fondé sur la *blockchain*.

La Défense en métropole

Sur le territoire métropolitain, les hauts standards de sécurité, tels que définis dans l'Instruction générale interministérielle 1300, sont plus aisément respectés qu'en opérations. Les infrastructures sont plus consistantes, les moyens pour les protéger (hommes, caméras, entraves) plus nombreux et les réseaux plus robustes. Ceci devrait faciliter un déploiement décentralisé de données traditionnellement centralisées, contrairement au cas des déploiements outre-mer évoqués plus haut. Plusieurs cas d'usage sont envisageables.

Le plus accessible est une évolution de solutions déjà utilisées. Il consisterait en une décentralisation de l'ensemble des processus administratifs ainsi que leur inscription dans un registre unique et transparent, auditable par tous. Les logiciels de signature électronique et de suivi de courrier, par exemple LNACRE pour l'armée de Terre, sont trop lourds et ne sont pas universels ; ils pourraient être remplacés par des solutions légères permettant l'accès à n'importe quel document officiel et son authentification instantanée.

En métropole toujours, se pose la question de la protection des actes confidentiels dits "spécifiques" (actes de chancellerie, confidentiel médical…). La pandémie Covid-19 a forcé au confinement l'ensemble des cadres militaires qui n'étaient pas employés sur des fonctions immédiatement opérationnelles. Pour autant, la vie administrative a suivi son cours, avec ses échéances imposées. Éloignés de leurs enceintes militaires sécurisées, les cadres s'en sont davantage remis à des solutions de communication à distance peu sécurisées, révélant à l'occasion la fragilité de cette organisation centralisée. En effet, la concentration sur certains serveurs de toutes ces données cruciales à la vie militaire est une vulnérabilité face à une panne d'envergure ou à une cyber-attaque qui aurait des conséquences importantes sur le fonctionnement d'une armée déjà contrainte d'adopter un fonctionnement "alternatif". Là encore, le choix d'une distribution décentralisée des données rendrait plus robuste l'organisation en permettant de toujours trouver un chemin vers l'information, même en cas de perte d'un ou plusieurs nœuds. La partie logicielle, quant à elle, permettrait des échanges chiffrés, donc la mise en place d'un écosystème de travail complet et sécurisé.

Dans les années 1960, les Américains avaient créé Arpanet, un réseau couvrant l'ensemble du territoire d'un maillage sans nœud central, dont l'ambition était de créer la capacité de communiquer à travers le territoire après une attaque nucléaire. Les évolutions d'Arpanet accouchèrent d'Internet tel que nous le connaissons aujourd'hui. Cependant Internet, tout comme les réseaux militaires, a peu à peu dévié vers une arborescence centralisée : des serveurs centraux distribuent l'information vers des ordinateurs clients en grappe autour d'eux, devenant ainsi des points de vulnérabilité.

Le déploiement d'une solution totalement décentralisée mériterait d'être envisagée pour l'ensemble des capacités concourant à la défense du territoire national. Les satellites de surveillance, les moyens de défense sol-air, les aéronefs d'alerte mais aussi les unités engagées en cas de catastrophe naturelle, voire "NRBC", devraient être dotées d'un réseau totalement décentralisé capable d'assurer la pérennité de la mission de protection une fois

le premier choc encaissé. Le récent *hackathon Blockchain*[30] organisé par le ministère des Armées à Palaiseau pourrait être un premier pas dans cette direction. Son succès permettra le développement de premiers cas d'usages spécifiques qui, espérons-le, contribueront à démocratiser cette technologie.

Par ailleurs, la très forte territorialisation des Armées permet d'envisager aisément le déploiement généralisé de l'équipement nécessaire à ce type de réseau en autonomie. La paralysie du monde entier suite à la propagation d'un virus si peu létal ne doit pas occulter le risque plus grand que revêtirait un virus plus mortel, voire un *blackout* complet suite, par exemple, à une cyber-attaque de grande ampleur. L'épisode Covid-19 nous rappelle qu'entrapercevoir les déclencheurs d'une crise et ses conséquences n'est pas suffisant sans préparation. Il faut dorénavant consentir le coût matériel de la résilience.

Que font les forces de l'OTAN ?

Premiers programmes

Parmi nos alliés, l'intérêt pour la *blockchain* se manifeste aussi. Les forces américaines, toujours dans la crainte d'un déclassement stratégique, poursuivent leur politique d'investissements massifs dans les nouvelles technologies. De plus, on ne peut ignorer le renforcement de la rhétorique guerrière apparue à la suite des multiples frictions avec les forces russes sur le théâtre syrien, ou chinoises en Mer de Chine. Outre le déploiement d'un *cloud* sécurisé et l'utilisation de l'intelligence artificielle dans l'aide à la prise de décision, les Américains ont souhaité se doter d'une capacité à échanger de l'information de façon sécurisée dans un environnement contesté. C'est ce que vient confirmer l'évocation de la *blockchain* dans le plan budgétaire de 700 milliards de dollars voulu par le Président Trump en 2017. Par ailleurs, la DARPA expérimente depuis 2016 un protocole de messagerie décentralisé fondé sur cette technologie. Ensemble indissociable, ces technologies constituent le cœur des réformes de modernisation entreprises outre-Atlantique pour s'assurer la suprématie opérationnelle lors des chocs qu'on voit venir.

Pourtant, l'approche de la DARPA émettant en 2019 une demande d'information sur les capacités de la *blockchain* dans l'amélioration de la sécurité, du stockage ou du calcul devrait inquiéter. Loin de témoigner d'un intérêt supérieur pour cette technologie, elle révèle davantage de la méfiance, voire de l'incompréhension. Or, venant de l'agence de R&D et de prospective de l'armée au plus fort budget au monde, celle qui a créé Internet, le wifi et le GPS, il y a de quoi s'interroger face à cette incapacité à penser des cas d'usages stratégiques. D'autant plus que la (maigre) littérature sur le sujet laisse deviner une approche beaucoup plus audacieuse de la part de la Chine et de la Russie. La première n'a pas ménagé les annonces de ses hauts dignitaires militaires quant à l'intérêt stratégique du Parti pour cette technologie et a, par exemple, évoqué la création d'un crypto-Renminbi. La seconde a dévoilé son projet d'un réseau de cyberdéfense fondé sur la *blockchain* pour mieux permettre la traçabilité des attaques et leur attribution.[31]

---

[30] *Cf.* https://www.defense.gouv.fr/actualites/articles/grande-reussite-pour-le-premier-hackathon-blockchain.

[31] Sur ces sujets, voir : https://media.consensys.net/why-military-blockchain-is-critical-in-the-age-of-cyber-warfare-93bea0be7619 et https://iz.ru/758288/nikolai-surkov-aleksei-ramm/blokchein-odenut-v-kamufliazh.

Concernant l'OTAN, son état-major tentaculaire, le SHAPE (*Supreme Headquarters Allied Powers Europe*), a vocation à penser la standardisation, indispensable à l'inter-opérabilité de ses membres. C'est ainsi que fut créé le calibre 5.56 mm pour les fusils d'assaut afin de faciliter la logistique, ou qu'ont été pensés les messages simplifiés d'évacuation sanitaire pour accélérer la prise en charge des blessés au combat. Mais qui s'intéresse à l'interopérabilité devrait s'intéresser à la *blockchain* ! En effet, la création d'une architecture informatique unique et sécurisée pourrait devenir la colonne vertébrale de l'échange d'informations. Or, cette capacité devient cruciale dans l'ère de la guerre de l'information !

Le propre des opérations de l'OTAN étant le travail multilatéral, en coalition, on devine que le volume de données échangées quotidiennement est phénoménal. Si le travail hors-coalition autorise certains raccourcis dans les procédures (par la force de l'habitude et la connaissance partagée), le travail collaboratif, sitôt qu'il implique plusieurs nations, passe par d'innombrables phases de contrôle de conformité générant autant de données essentielles.

La *NATO Communication and Information Agency*, en charge de la stratégie des moyens de communication de l'Alliance, a lancé en 2016 un appel à projet pour des solutions *blockchain*. Sa formulation ne laisse pourtant malheureusement que peu d'espoir pour de vraies applications stratégiques. Les propositions relèveront sans doute davantage de la messagerie et du suivi logistique que du projet d'envergure. Pourtant, une plus grande ambition dans la recherche d'efficacité et de robustesse aurait pu pousser à envisager la création d'un réseau permettant de valider rapidement la conformité à la doctrine d'ordres d'opérations ainsi que leur inscription de façon immuable dans un registre facilement auditable par tous ceux présentant les habilitations nécessaires.

La démarche de M. Rasmussen

En mars 2019, Anders Fogh Rasmussen, ancien Premier ministre du Danemark et surtout ancien Secrétaire général de l'OTAN (2009-2014), a rejoint, en tant que conseiller stratégique, une start-up basée en Suisse et spécialisée dans les *blockchains* en rapport avec l'identité : Concordium.[32] Comme dans le cas de M. Noyer, ancien gouverneur de la Banque de France, parti quelques semaines plus tôt rejoindre le Conseil d'administration d'une start-up spécialisée dans les solutions *blockchain* destinées aux marchés financiers, la démarche mérite d'être regardée de près en raison du profil de M. Rasmussen.

Concordium a été fondé par Lars Seier Christensen, qui avait également fondé Saxo Bank et en était auparavant le PDG. La jeune entreprise construit ce qu'elle décrit comme un réseau de *blockchain* conforme à la réglementation et validant l'identité (ID) et la connaissance du client (KYC). La société avait lancé en 2019 une preuve de concept du service et prévoyait un lancement public complet au premier trimestre 2020.

Selon M. Christensen, Concordium prévoyait de se lancer dans des domaines qui nécessitent une solution *blockchain* pour "*les communications privées et sécurisées, ainsi que la liaison avec les départements gouvernementaux*". Un vocabulaire un peu martial,

[32] Voir : https://concordium.com/.

donc, même si le réseau de Concordium doit aussi permettre des systèmes de vote "inviolables" afin de "*protéger les institutions de la société civile, qui sont fondamentales pour le fonctionnement de la démocratie*".

M. Rasmussen lui-même insiste sur certains types de bénéfices :

> Nous commençons seulement à voir les avantages que la technologie de la chaîne de blocage apportera à nos sociétés, y compris dans nos processus démocratiques. La solution de vote de Concordium offre un moyen de vote fiable, rapide et économique.

Mais il est patent que Concordium vise à combiner sa fonction intégrée de lutte contre le blanchiment d'argent (AML) et de contrôle des clés (KYC) avec une technologie de protection de la vie privée à connaissance zéro et la conformité avec le Règlement général sur la protection des données (RGPD). Enfin, ce projet développe également une monnaie cryptographique appelée GTU (Global Transactions Unit), également dotée d'une fonction de conformité intégrée. On a déjà dit que c'était là une chose que les militaires pourraient un jour considérer.

Identité numérique : l'exemple estonien

Outre les usages tactiques abordés, une autre avancée mériterait d'être étudiée plus à fond. On le voit, la numérisation suit son cours et avec elle se pose la question de la confiance dans l'éther des échanges dématérialisés. Y reproduire le concept d'identité numérique semble une idée qui arrive à maturité.

Aux critiques militant pour un Internet libre et anonyme, on peut répondre qu'il existera toujours et que cela dépend d'abord d'eux-mêmes. Cependant, certains services, notamment ceux qui relèvent de la sécurité, devraient se faire après vérification que l'usager est bien celui qu'il prétend être. Rien ne semble empêcher la coexistence de l'anonymat actuel et de l'identité. L'Estonie, pays membre de l'Alliance atlantique, fait figure de précurseur dans ce domaine : ayant fait le choix du tout numérique au milieu des années 90, 99% de ses services sont dématérialisés. On peut y payer ses impôts, recevoir son ordonnance et réaliser ses démarches sociales en ligne. Pour cela, chaque Estonien se voit doté d'une carte à puce (et de son petit lecteur USB) qui fait office de carte d'identité, de permis de conduire, de carte vitale et d'abonnement pour les transports en commun.

Sans aborder ici les bienfaits d'une approche globale dépassant le seul aspect militaire, l'identité numérique permettrait des échanges de confiance entre personnes ainsi dotées. Que ce soit des cartes à puce ou des clefs USB (FIDO, type YUBIKEY permettant une validation cryptographique), cela réduirait dans tous les cas les possibilités de cyber-attaques de nos ennemis. Or, la question de la confiance étant au cœur de la technologie *blockchain*, il apparaît naturel de loger l'ensemble de ces services d'identification/ validation au sein d'une *blockchain* qui pourrait être interrogée par n'importe quel service ayant besoin d'authentifier un usager.

Les défis à relever

L'état des lieux qui vient d'être tracé montre le pragmatisme, et l'intérêt réel, des militaires. Il faut tout de même souligner que, dans chaque secteur, il est le fait de profils particuliers (et pas forcément majoritaires). Du côté de la finance, tous les *bitcoineurs* le

diront : ce qui rend leur monnaie passionnante, et non simplement intéressante, c'est l'ampleur des remises en cause, des changements de perspectives ou de paradigmes qu'elle suscite en et parmi eux. La *blockchain* est à cet égard comparable. Parmi les militaires, elle intriguera d'abord ceux qui font le pari de faire des paris. Il leur faut alors lever les doutes autour d'eux, réfuter les craintes liées aux usages illicites des crypto-monnaies, trouver les mots pour faire admettre de nouvelles idées, pour rapprocher parfois deux mondes qui ont à apprendre l'un de l'autre, pour faire comprendre que la *blockchain* n'est pas un gadget pour informaticien mais une arme dans le cyberespace, voire sur le terrain.

Les utilisations malhonnêtes, terroristes ou criminelles

Les risques fantasmés et les vrais

L'existence d'une face sombre des crypto-monnaies est-elle une bonne raison d'ignorer la *blockchain* ou d'en parler comme si le sujet était entièrement distinct ? Pas une déclaration publique sur la *blockchain* n'a fait l'économie soit d'une affirmation, jamais fondée scientifiquement, pour distinguer la *blockchain* de *Bitcoin*, soit de laborieux distinguos visant à ôter le venin à la créature anarchiste pour en faire une docile amie de l'ordre. Dans les 2 cas, *Bitcoin* est "sulfureux". Et comme être anarchiste, après tout, n'est pas interdit, il est carrément "criminel".

Que le *bitcoin* ait attiré l'attention de la crapule ne fait pas de doute. Le règlement des transactions restait en 2009, le maillon faible des activités illégales dans le *darknet*. Que les acteurs des marchés illégaux aient compté parmi les premiers utilisateurs du *bitcoin* s'explique donc aisément. Pour bien le comprendre, il faut écouter Michel Koutouzis, historien-ethnologue spécialisé sur les questions de trafic et de blanchiment:

> Si une structure agit au sein du monde tel qu'il est, et non pas tel qu'il est souhaité ou décrit, c'est bien les mafias. Leur angle de vue, lointain et lucide à la fois, scrute la globalisation, reste à l'affût de nouveaux espaces, s'intègre dans notre vie de tous les jours.[33]

Est-ce une provocation, maintenant, que de soutenir que les mêmes innovations concernent aussi précocement des militaires ? Les uns comme les autres sont à l'affût de la disruption qui va permettre de réaliser un "coup" jamais vu ou de "percer le front".

Fin 1910, la "bande à Bonnot" utilise une De Dion-Bouton pour semer policiers et gendarmes qui se déplacent encore à cheval ou à vélo. Bonnot suit de près, lui, l'évolution de la technique. Il s'informe des différents modèles. Le 21 décembre 1911, il choisit une limousine Delaunay-Belleville de 12 CV, marque de luxe qu'il sait fiable et rapide, pour réaliser contre la Société Générale le premier "casse" en automobile de l'histoire. Mais en 1914 le général Gallieni, en réquisitionnant les fameux "taxis de la Marne", trouve lui aussi une manœuvre inédite qui eut une réelle portée psychologique. L'automobile ne deviendra un moyen de transport de masse que bien plus tard.

Comme pour la *blockchain*, on a dit à l'origine d'Internet qu'il ne servirait à rien (*cf*. le fameux rapport Théry[34] de 1994), ou seulement aux criminels. Et Internet a servi aux

---

[33] *Cf*. "La guerre anti-blanchiment n'aura pas lieu", publié dans la revue *Chimères*, n°91, novembre 2017.
[34] *Cf*. https://www.vie-publique.fr/sites/default/files/rapport/pdf/064000675.pdf.

criminels. Si une invention ne sert pas aux criminels (surtout dans ses premiers pas), c'est probablement qu'elle n'apporte rien. Refuser de s'en servir pour ce motif est une sottise, d'autant que c'est souvent se laisser impressionner par les arguments des lobbies industriels du passé que cette invention menace, et donc prendre le risque de combattre avec des canons de bronze se chargeant encore par la gueule un ennemi bien équipé en canons d'acier de chez Krupp.

À ce jeu, les militaires ne sont d'ailleurs pas forcément "suiveurs": le routage "en oignon" (TOR) n'a pas été développé pour faire circuler de façon anonyme du contenu pédopornographique (ce qu'il fait, hélas, sans conteste), mais en partie par des militaires américains pour augmenter la sécurité de leurs communications, fonction qu'il assure aussi d'ailleurs au bénéfice de communications civiles, comme celles de la presse et de certaines "sources" dont l'existence serait menacée par des communications traçables.

Ceci posé, le poids réel des crypto-monnaies dans les activités illégales, lorsqu'il est chiffré, est généralement moins spectaculaire que ce que les gros titres de presse laisseraient penser. Pour la drogue, il a sensiblement reculé depuis 2012. La capitalisation même de ces monnaies est, malgré la hausse depuis lors, bien insuffisante pour en faire un instrument adéquat de ce trafic dont les méfaits se mesurent en trillions. D'une manière générale, en 2019, seulement 0,5% du total des transactions en *bitcoins* (soit 829 millions de dollars) aurait été dépensé dans le *darknet.*[35] Régulièrement cité comme instrument du financement islamiste, le *bitcoin* s'avère également d'un faible concours ici : le groupe Al-Sadaqah n'aurait par exemple récolté que 1037 de dollars en un an et demi et si les transactions du Hamas ont atteint près de 1000 de dollars en quelques jours, elles ont toutefois été très rapidement "tracées". Enfin, les rançons en *bitcoins* du *ransomware* planétaire "Wanna Cry" n'avaient, en 2017, pas dépassé 55 *bitcoin*s.

Le coût des parades

L'incantation n'est pas une parade. L'interdiction (comme celle de l'arbalète par le concile de Latran en 1139) non plus. En outre, celui qui organise un crime est rarement rebuté par l'illégalité d'un protocole informatique, pas davantage que d'une arme ou d'une monnaie. La seule parade, comme les spécialistes de la Gendarmerie nationale l'ont montré en appréhendant des cybercriminels, c'est une connaissance fine de la technologie.

Au niveau international, Europol est l'une des organisations policières qui s'est intéressée très tôt à la formation des policiers en matière de *bitcoin* et de crypto-monnaies en général. Son *European Cybercrime Centre* (ou "EC3") organise depuis 5 ans des conférences annuelles sur les monnaies numériques dont la 5e édition, les 19-21 juin 2018, à La Haye, fut la plus grande réunion européenne des forces de police réunissant plus de 300 participants venant de 40 pays autour de sujets comme la traçabilité et le dé-mixage des transactions.

Si pour remonter les filières, démonter les réseaux, traquer les rançons et anticiper les coups à venir (monnaies plus anonymes, "laveries" crypto, etc.) mieux vaut être

[35] *Cf.* https://www.elliptic.co/our-thinking/bitcoin-money-laundering.

docteur en informatique, mieux vaut aussi travailler en partenariat avec des start-ups qui développent d'utiles instruments. Comme le remarque Maître Michelle Abraham[36] :

> L'échange de bonnes pratiques entre les instances de police internationales et les sociétés Bitcoin est essentiel. Cet échange a été possible dans la mesure où ces sociétés ont été les premières victimes des cybercriminels.

D'autre part, les principales plateformes de change ont adopté en majorité un système d'autorégulation par lequel elles se soumettent déjà volontairement à un certain nombre de règles du secteur financier concernant les dispositions anti-blanchiment et anti-terrorisme. Il y a donc des bases de réelle convergence pratique entre les forces de l'ordre et l'industrie crypto. Des représentants d'entreprises du secteur[37] étaient présents à la conférence d'Europol, qui les décrit comme des experts-clés du monde des crypto-monnaies, travaillant main dans la main avec les forces de l'ordre.

Plusieurs start-ups ont développé des solutions de traçage, mises à disposition des services de police comme des industriels. Ainsi, la luxembourgeoise Scorechain fut ainsi parmi les premières à proposer un explorateur de blocs qui permet aux entreprises devant mettre en place des procédures KYC (*know your customer*) et AML (*anti-money laundering*) de générer des rapports d'analyse avancés afin d'évaluer les risques liés à une transaction *Bitcoin*. Basée à Londres, la start-up Elliptic s'était d'abord spécialisée dans la production d'une solution de coffre-fort numérique (*vault*) hors-ligne ; elle a depuis acquis une position importante dans le traçage.

Il s'agit d'un domaine en constante évolution (en mai 2019, le ministère de l'Intérieur lançait un appel d'offre sur ce thème[38]) et qui suscite de nombreuses rencontres. Parmi les espaces créés à cet effet, le Forum International de la Cybersécurité (FIC) s'est imposé comme l'événement de référence en Europe en matière de sécurité et de confiance numérique. Son originalité est de mêler (en janvier à Lille) un Forum annuel favorisant la réflexion et l'échange au sein de l'écosystème européen de la cyber-sécurité et un Salon dédié aux rencontres entre acheteurs et fournisseurs de solutions de cybersécurité.[39] Partenaire historique, le ministère des Armées s'associe chaque année à ce rendez-vous incontournable.[40]

L'arsenal cyber des États étrangers potentiellement hostiles

Si l'on examine ce qui transpire chez de grands États non-membres de l'OTAN, on voit que le débat (pour sa "partie émergée") reste centré sur la licéité de l'usage monétaire, entre crainte de dollarisation (via *Bitcoin* ou *Libra*) et tentation d'une cryptomonnaie

---

[36] *Cf.* l'article déjà cité : https://bitcoin.fr/les-gendarmes-les-voleurs-et-bitcoin-2-2/.

[37] À savoir : Bitcoin.de, Bitfinex, BitPanda, Bitstamp, BitPay, Blockchain.info, CEX, Coinfloor, Coinhouse [l'ancienne "Maison du bitcoin"], Cryptopia, Cubits, Kraken, LocalBitcoins, OKCoin, StectroCoin et Xapo.

[38] *Cf.* https://bitcoin.fr/analyse-de-la-blockchain-lappel-doffres-du-ministere-de-linterieur/.

[39] La V^{e} édition de son Agor@, organisée par la Gendarmerie en novembre 2018, s'était attachée à répondre aux questions évoquées ci-dessus, en recevant des législateurs d'influence, des experts de haut niveau et l'ambassadeur d'Estonie. En 2019, le FIC a reçu les deux "crypto-députés", Laure de la Raudière et Jean-Michel Mis.

[40] En 2020, il était représenté par le Commandement de la Cyberdéfense (COMCYBER), la DGA, la DRSD, la DRM, la DGSE, la DIRISI, les réserves de cyberdéfense et l'État-major des Armées.

permettant d'augmenter la surveillance et l'emprise sur la société. Cet intérêt pour les monnaies numériques baptisées "cryptographiques" par souci d'affichage, s'inscrit, dans certains pays dans des enjeux clairement stratégiques.

Ainsi, les Chinois s'intéressent de près et depuis longtemps à la *blockchain* pour son aspect cryptomonétaire. Couplé à leur internet fermé, c'est un nouveau modèle qui est en train de naître en Extrême-Orient. Le Venezuela, pour sa part, utiliserait [41] un portefeuille digital pour transformer les recettes issues des taxes des aéroports domestiques en crypto-monnaies ensuite transférés à Hong-Kong, en Chine, en Russie ou en Hongrie, où elles seraient converties – manœuvre permettant surtout aux autorités vénézuéliennes de contourner les sanctions économiques à leur encontre. L'Iran, lui-même soumis à un blocus de cet ordre, aurait lancé en juin 2019 une "cryptomonnaie" adossée à la réserve d'or iranienne.[42] Quel que soit l'avenir de cette monnaie, les Iraniens semblent s'intéresser à la *blockchain* comme parade – ce serait une première ! – à cette arme polyvalente et de précision qu'est le dollar. La Russie et la Turquie auraient réalisé en décembre 2017 une transaction portant sur du blé, uniquement grâce au *Bitcoin*.[43]

Au-delà des stratégies monétaires, les sujets militaires, ne doivent évidemment pas être absents, même s'ils sont moins souvent mentionnés publiquement que ceux de santé ou de logistique. La Russie, par exemple, a investi un milliard d'euros dans les recherches autour de la *blockchain.*[44] Ce qui confirme qu'elle envisage bien de "*blockchainiser*" sa cyberdéfense pour optimiser la traçabilité d'attaques futures.

Les autres nations dites hostiles ont soit maintenu le secret sur leurs projets, soit ne se sont pas emparés de ce sujet.

Riposte et guerre des cerveaux

Les nations occidentales, après une montée en puissance du Cyber depuis une quinzaine d'années, continuent à explorer les technologies capables de leur assurer un avantage comparatif. Sans surprise, on constate que l'intelligence artificielle (IA) concentre l'essentiel de l'attention et sans trahir de secret, on retrouve parmi les nations qui comptent et qui s'intéressent au sujet, les États-Unis, Israël ou la France. Se doter, grâce à l'intelligence artificielle, d'une capacité à détecter et anticiper des attaques serait un atout pour qui en serait muni, car le cyberespace est devenu un champ de confrontation où l'origine des attaques est difficilement attribuable et où les dommages peuvent être conséquents.

Toutefois, les avancées actuelles sur l'intelligence artificielle relèvent davantage de l'exercice d'une communication bien rodée que de la vraie percée technologique. Dans ce

---

[41] Voir entre autres, à ce propos : https://www.abc.es/internacional/abci-maduro-tasas-aeroportuarias-para-burlar-sanciones-eeuu-201907212232_noticia.html?ref=https%3A%2F%2Fomc.ceis.eu%2Fgeopolitique-de-la-blockchain%2F.

[42] *Cf*. https://www.ccn.com/iran-punks-trump-crypto/.

[43] C'est ce que rapporte l'Agence Bloomberg : https://www.bloomberg.com/news/articles/2018-01-23/first-cryptocurrency-freight-deal-takes-russian-wheat-to-turkey.

[44] Sur ce sujet : https://www.thecointribune.com/actualites/les-milliards-que-la-russie-compte-gagner-avec-ses-investissements-blockchain/.

domaine, secteurs public et privé sont en compétition pour attirer les talents. Or, si certaines missions régaliennes peuvent avoir un réel lustre auprès de jeunes scientifiques "pointus", la puissance publique n'est pas en mesure d'être très concurrentielle au plan matériel.

Les assistants vocaux sont souvent présentés comme la partie visible de l'IA. Ils seraient une étape intermédiaire avant les vraies IA, faible puis forte, décrites par Laurent Alexandre. Or, lorsqu'on voit les capacités réelles des *Siri*, *Cortana* ou *Alexa*, malgré un investissement R&D total de 54 milliards de dollars pour Apple, Microsoft et Amazon, on peut légitimement s'interroger et, dans un raccourci rapide, se demander comment les divisions recherche des bases industrielles de technologie et de défense, avec leurs moyens humains et matériels plus limités, pourraient développer des outils capables de nourrir les attentes créées par Hollywood et ses films. L'industrie de l'IA est aujourd'hui plus une industrie de la promesse que du résultat.

En regard, la *blockchain* pourrait être amenée à prendre une place prépondérante en apportant des résultats opératoires concrets. La technologie est mature et de nombreux cas d'usages sont d'ores et déjà accessibles. L'obstacle à l'adoption professionnelle de celle-ci relève pour l'essentiel, comme on va le voir, de sa complexité. Si celle-ci est maîtrisée, il n'est alors pas irrationnel d'imaginer que cette technologie connaisse une adoption plus rapide et visible que l'intelligence artificielle. Si tel est le cas, du Proche à l'Extrême-Orient, nos adversaires ayant fait le choix d'investir dans cette technologie auront une longueur d'avance dans la compétition mondiale et dans le jeu des puissances.

La "continuation de la politique"

Si la *blockchain* est, comme tout l'indique, à ranger parmi les armes conçues pour lutter contre les banques, utiles aux gendarmes comme aux voleurs, elles sont comme les baïonnettes avec lesquelles, selon Talleyrand, on pouvait tout faire sauf s'asseoir dessus. Il faut que la *blockchain* soit rendue compréhensible aux militaires, admissible par l'opinion publique et qu'elle soit consolidée par les savants.

Rendre compréhensibles par les militaires des choses contre-intuitives

On ne va pas revenir ici sur les obstacles mentaux liés à la réputation dite "sulfureuse" de *Bitcoin*. Face à un public militaire, il y a au moins deux sujets à "déminer": celui de la décentralisation des données et celui, d'ailleurs connexe, de leur ouverture au public. Ils ont été abordés plus haut, dans le court historique qui ouvre cet article. Il reste à trouver les moyens de les présenter au mieux non à des informaticiens un peu anarchistes, mais à des militaires plutôt habitués à la hiérarchie.

Or, dans la hiérarchie des secrets, le "secret Défense" est à certains égards mieux défendu que le secret d'État.[45] Comme les banquiers pour leur or, les militaires ont

[45] Plusieurs indices permettent de le mesurer, dont la conservation par les Armées elles-mêmes de leurs propres archives. Alors que celles de l'Élysée et des ministères sont versées aux Archives nationales, les trois Armées ont jalousement conservé chacune leurs fonds jusqu'en 2005. Un autre en est le peu d'influence que l'Europe parvient à exercer sur ce domaine de compétence souveraine.

longtemps compté sur le béton et le blindage pour protéger leurs secrets, développant de ce fait une sorte de "culture du coffre-fort", que les réalités numériques viennent bousculer.

Avec l'accumulation des données chez les "géants" du Net a crû aussi l'ampleur des vols de données, clés secrètes, identités, profils : 68 millions chez Dropbox, 117 millions chez LinkedIn, 145 millions chez Ebay et (record en 2016) 500 millions de profils Yahoo. Sans faire de leur discrétion assurée un argument publicitaire explicite comme le faisait imprudemment le site de rencontres extraconjugales Ashley Madison (40 millions de profils volés), tous ces sites prennent des précautions et se vantent à l'occasion d'une sécurité "*de niveau militaire*".

Le film bien connu *Goldfinger* suggère de façon concrète le risque inhérent au fait de conserver tous ses œufs, tous ses lingots, toutes ses munitions…ou tous ses secrets dans le même coffre-fort. Ranger les avions aile contre aile (par peur du sabotage) comme à Pearl Harbor peut aussi s'avérer tragique. Il faut comprendre que, comme les parasites naturels attirés par la monoculture intensive sur des milliers d'hectares, les *hackers* sont objectivement stimulés par l'entreposage compact de millions de téraoctets de données valorisables.

Avec un fonctionnement disséminé, où chaque émetteur ou possesseur de données secrètes les conserve, n'inscrivant dans le fichier commun qu'est une *blockchain* publique (comme dans le cas du gendarme évoqué plus haut) qu'une "preuve" chiffrée, de façon à authentifier, en cas de besoin, le moment venu et devant l'autorité compétente, la validité de sa pièce justificative, les prédateurs naturels perdent l'avantage.

Cependant le caractère "public" des grandes *blockchains* (*Bitcoin* mais aussi *Ethereum*, *Tezos*, etc.) est également contre-intuitif. Qui ne préfèrerait garer sa voiture au 3^{e} sous-sol, dans son box fermant à clé, plutôt que dans la rue, portes ouvertes ?

Il faut ici expliquer d'abord qu'une menace légère sur le concierge et un pied-de-biche suffisent amplement à détruire l'illusion de sécurité dans la première option, ensuite que la seconde option est un peu plus complexe. Certes, l'automobile va stationner au vu et au su de tous, portes ouvertes, sur la place du village. Mais une seule personne (son propriétaire) en détient la clé. Les gens du village ignorent son nom, mais un registre permet de vérifier qu'il n'existe qu'une clé et que son porteur est légitime. Pour passer outre, il faudrait un vote d'une majorité des habitants, dont les propres voitures sont garées dans les mêmes conditions, et qui risquent le vol ou la confiscation de leurs propres voitures en cas de vote malhonnête…

Remplaçons au besoin l'automobile par un blindé, les habitants par les chefs de corps d'une même armée et nous avons le fonctionnement d'une *blockchain* de type "consortial", qui pourrait en l'occurrence être lisible par tout homme en uniforme, et dont les mouvements seraient validés, non pas tous depuis un unique état-major, mais par un nombre suffisant de cadres militaires habilités et dispersés sur le territoire.

Rendre la* blockchain *socialement acceptable dans un cadre démocratique

L'opinion, dans un état démocratique, n'est pas une chose cristalline. Il y a du conflit, et il y a du changement. Tout ce qui a affaire aux libertés individuelles d'une part, à la sécurité publique d'autre part, demande un réglage fin. Bien sûr, les avancées

(spectaculaires depuis des années) des éléments de surveillance ont été permises par l'état d'urgence et son infusion progressive dans la loi ordinaire, au fil des attentats terroristes récurrents, et malgré quelques coups d'arrêts portés par le Conseil d'État ou la CNIL, par exemple. Si l'on excepte des protestations de principe souvent marginales et généralement impuissantes, la chose semble plutôt n'irriter l'opinion que lorsqu'elle s'avère rétrospectivement inutile.

L'épisode pandémique actuel, occasion d'une nouvelle loi d'urgence élargissant considérablement le nombre des "suspects", pourrait cependant poser des problèmes nouveaux. Comme cela a été très vite remarqué, il semblerait peu compréhensible d'assigner à résidence quelqu'un qui a croisé dans le métro une personne testée, ou même cette dernière si elle ne souffre pas de symptômes particuliers, quand des radicalisés "fichés S" sont laissés en liberté. Au reste, dans un cas comme dans l'autre, l'ingénierie humaine (nombre de fonctionnaires chargés de la surveillance, de l'application, de la punition, etc.) et le consentement des citoyens (voir les polémiques et rumeurs en ligne autour de la "prime de 2 euros") suggèrent des limites à ces dispositifs.

La technologie de la *blockchain*, justement parce qu'elle n'implique pas de mettre toutes les données *en clair* dans un unique silo, où elles finiront fatalement par être conservées plus longtemps que prévu, être vues par trop de gens (intrus compris) et être exploitées peut-être à d'autres fins, pourrait fournir un compromis acceptable entre l'impératif de santé et respect de la vie privée.[46]

Cette thématique n'a aucune raison d'être étrangère aux militaires qui ont eux-mêmes, en tant que tels, une relation spéciale à la protection de la vie personnelle.[47] La suppression des tribunaux militaires pour le temps de paix (1982) puis du Tribunal aux Armées de Paris (2012) a considérablement réduit l'écart par rapport au droit commun en ce qui les concerne et leur exposition à de possibles poursuites (de victimes ou bien de familles de soldats tombés en opération).

D'autre part les militaires, en hommes de leur temps, ne sont pas absents sur Internet, où l'antique obligation de réserve a connu un notable assouplissement, avec la quasi-disparition du régime d'autorisation préalable pour s'exprimer, un recours probable à l'anonymat des forums, mais aussi des blogs parfaitement revendiqués et identifiés tenus par des cadres. La Délégation à l'Information et à la Communication de la Défense a publié en 2012 un guide pédagogique intitulé *Guide de bon usage – Média sociaux*, renouvelé en 2016,[48] qui fait sa part à l'esprit du temps.

---

[46] On peut noter que dans l'article documenté et laissant une part aux objections qu'il consacre à ce sujet, le Secrétaire d'État au Numérique, M. Cédric O, exprime finalement une préférence pour ne conserver, dans le cas de l'application StopCovid, que des données chiffrées, mais sauvegardées dans un silo centralisé (https://medium.com/@cedric.o/stopcovid-ou-encore-b5794d99bb12). D'autre part, il est fort probable que les fichiers constitués par les "brigades de santé" seront finalement stockés en clair, avec les garanties usuelles apportées par l'Assurance Maladie.

[47] Bertrand Quaglierini, *Le militaire : entre citoyen, agent public et soldat*, Université d'Avignon (Droit), 2017. En ligne à l'adresse : https://tel.archives-ouvertes.fr/tel-01753376/document. Le chapitre 1 du Titre 3 de la Partie II traite notamment de la protection face aux désagréments liés à l'activité des militaires.

[48] *Cf.* notamment, Livre 1, Titre 2, chapitre 3 "Une liberté d'exprimer ses opinions en dehors du service", et https://www.defense.gouv.fr/actualites/articles/sortie-du-nouveau-guide-du-bon-usage-des-reseaux-sociaux.

Conforter la collaboration avec les savants nationaux

Les relations entre les militaires et les universitaires sont une chose généralement peu médiatisée. Commençons par les écoles et instituts internes à la Défense. L'IRSEM (Institut de recherche stratégique de l'École Militaire), organisme extérieur de la DGRIS, *think-tank* doté d'un conseil scientifique composé notamment de juristes ou d'historiens, et où se retrouvent de nombreux doctorants à profil très "Sciences Po", produit essentiellement des notes sur des sujets de géostratégie, et la *blockchain* en semble absente. À l'École Militaire encore, l'IHEDN (Institut des hautes études de Défense nationale), semble à ce jour avoir peu abordé la question. En revanche, à l'École de Guerre, le mémoire du chef d'escadron Cécile Lambert, officier stagiaire de la 26e promotion, était consacré en mars 2019 à "La technologie *blockchain* et son côté disruptif pour de multiples applications futures". Enfin, l'Enseignement Militaire Supérieur Scientifique et Technique (EMSST) est chargé de la mise en formation d'officiers supérieurs auprès des grandes écoles françaises, essentiellement scientifiques (malgré la présence d'écoles de commerce). C'est ainsi que chaque année, une trentaine de chefs de bataillon suivent des mastères spécialisés à Télécom Paris, Centrale Supélec ou Polytechnique. Les majeures suivies sont assez diverses mais, par le développement d'une culture scientifique et du réseau qui l'accompagne, ces hommes et femmes apportent aux Armées une capacité à s'emparer de sujets technologiques pointus avec les armes nécessaires à leur analyse.

À l'extérieur du périmètre des Armées, le Groupe Thalès, dont les activités Défense et Sécurité représentent 60% des activités, a noué des partenariats plus ou moins formalisés avec les Écoles Normales Supérieures de la rue d'Ulm (où il finance des thèses par des bourses), de Lyon ou de Saclay, institutions marquées par la figure de Jacques Stern, père de la cryptologie française. L'examen de nombreux CV sur le site LinkedIn permet de mesurer cette proximité.

Dans un autre registre, des contacts et échanges intellectuels existent dans un cadre à la fois érudit et convivial au sein d'une institution originale, l'Association des Réservistes du Chiffre et de la Sécurité de l'Information.[49] On rencontre à l'ARCSI des savants comme Jean-Jacques Quisquater, professeur émérite à l'Université Catholique de Louvain et fondateur de son Crypto Group, qui fut l'un des moteurs de la sécurité cryptographique et physique des applications de la carte à puce, mais aussi l'un des précurseurs de l'enseignement de la cryptographie à l'ENS et à l'X, avec Jacques Stern et Christine Nora…et l'un des 5 noms cités dans le *white paper* du mystérieux Satoshi Nakamoto.

Comprendre le terrain et les règles

Une fois que le stratège réfléchissant sur la révolution qu'apporte la *blockchain* est sorti de la logique du "château fort", il doit, s'il en poursuit l'étude dans une optique liée à

[49] L'ARCSI, tout en ayant conservé son nom d'origine (1928) "*entend conserver son lien privilégié avec le ministère de la Défense tout en s'ouvrant à tous les milieux professionnels, publics et privés, ayant à traiter de la protection des systèmes d'information et participant directement ou indirectement à la défense de notre pays et de son patrimoine*". Elle est présidée par le général (2s) Jean-Louis Desvignes, qui fut officier chiffre à l'État-major des Armées de 1985 à 1990 et chef du service central de la sécurité des systèmes d'information (aujourd'hui l'ANSSI) de 1995 à 2000.

la Sécurité publique et à la Défense nationale, envisager trois axes de réflexion : sur ce qui touche au terrain dans lequel se déroulent les échanges et les rencontres, sur les traces, les indices, les preuves qui en résultent et enfin sur la maîtrise nécessaire de tous les "langages" impliqués dans ces échanges.

Territoire et *Cloud*

On désigne traditionnellement par le terme "souveraineté" l'exercice d'un pouvoir, supérieur à tout autre, sur une zone géographique ou sur une population. La souveraineté, qui dans l'esprit issu des Traités de Westphalie, est le propre des États, s'inscrivait d'abord dans leur territoire. Mais elle a tendu à être prolongée dans les espaces maritime, aérien et désormais numérique, impliquant partout l'exclusion et la non-ingérence d'acteurs extérieurs dans les processus de gouvernement.

Dans l'espace numérique où se déploient les *blockchains* et leurs *smart contracts*, le premier facteur de souveraineté tient à l'existence d'une capacité "nationale" d'entretien, d'amélioration et de mise à jour du protocole-source, mais également de développement et d'audit des *smart contracts*. L'identification des ressources disponibles (centres de recherche, *clusters* technologiques, communautés de développeurs, etc.) ainsi que leur préservation, que ces dernières relèvent de compétences humaines ou d'écosystèmes d'entreprises, sont plus que jamais nécessaires. L'affrontement numérique passe ainsi par la promotion et le soutien apporté aux cerveaux et entreprises du pays.

La territorialité des infrastructures constitue un autre élément-clé de la souveraineté, en particulier pour la *blockchain*, dont le caractère distribué du stockage des informations, sous la forme de nœuds dispersés, ne l'affranchit pas pour autant de logiques territoriales. Unique ou multiple, le *storage* d'une base de données ne se fait pas hors-sol. Or, l'existence de dispositions législatives à caractère extraterritoriales – et notamment le *Cloud Act* américain – implique un audit préalable et scrupuleux de l'exposition d'une *blockchain* intéressant la souveraineté française aux intrusions et interférences étrangères. La gestion des nœuds doit également être examinée de près car un nœud n'est pas un dispositif passif. Une transaction validée (voire simplement compilée) par un nœud situé en territoire étranger peut être soumise à une loi différente de la loi française.

Big data, *identité et souveraineté*

L'identité des citoyens est au cœur du métier du gendarme. Pour le militaire (tant du moins qu'on ne lui demande pas de faire la distribution de produits rationnés), l'enjeu des notions abordées ici est essentiellement celui des failles dans sa souveraineté que la réalité numérique de notre pays provoque.

Ne serait-ce qu'en offrant la possibilité d'un système d'identité numérique robuste et de protection des données personnelles, mais pour bien d'autres raisons également, les *blockchains* peuvent contribuer à desserrer autour des données des Français l'étau des géants numériques, les GAFAM. Voyons donc ce qui se cache ici, en lieu et place de la pompeuse promesse d'*ubériser Uber.*

Les politiques se sont alarmés quand Facebook a publié son projet *Libra*. On pourrait sourire en songeant *Touchez pas au grisbi !*, comme l'auraient dit Albert Simonin, Jacques Becker ou Jean Gabin en leur temps, mais il s'agit plutôt d'une version

modernisée où le pari entre *le lièvre et la tortue* verrait le lièvre courir avec un sévère handicap derrière un troupeau d'éléphants.

La France a en effet un sérieux retard en matière de documents publics permettant de justifier de son identité dans l'espace numérique (et parfois dans la vie physique) :

- une carte nationale d'identité pratiquement inchangée depuis mars 1987, dont (en l'absence de puce) les éléments de "lecture numérique" sont dans la pratique réservés aux commissariats de police et aux bornes d'enregistrement aéroportuaires, mais que le citoyen ne peut nullement utiliser en ligne ;
- un système archaïque de justification de domicile (notion au demeurant un peu obsolète[50]) reposant presqu'entièrement sur des factures d'électricité dont la fiabilité est notoirement faible ;
- et en temps de pandémie et de parcimonieuses allocations de biens, une carte Vitale qui n'est ni universelle dans la population (les jeunes enfants sont inscrits sur celle de l'un des deux parents, ce qui ne va pas sans problèmes, tandis que les visiteurs étrangers et sans doute quelques marginaux en sont dépourvus) ou dans l'espace (la délivrance hospitalière est exclue du dispositif CPS), ni dans le temps puisqu'en cas de carte perdue, bloquée, ou dysfonctionnelle survient une carence, longue en temps normal et insupportable en période critique. Inversement, il en existe trop,[51] ce qui laisse penser que ses vertus pour l'allocation de biens rares et donc spéculatifs seraient minces. Enfin, cette carte dont les données sont sans doute loin d'être sécurisées de manière optimale, a régulièrement révélé différentes failles[52] évoquées dans plusieurs travaux parlementaires.[53]

Ce retard n'est évidemment pas moindre en ligne où, à la différence de ce qui peut être fait par exemple avec l'*e-card* estonienne, le citoyen français doit encore, en de nombreuses occasions, saisir lui-même ses données, scanner et uploader diverses pièces.

En pratique, il existe plusieurs procédés d'identification hors démarches officielles. Ceux mis en place par Facebook et Google, sont extrêmement *user-friendly* (pratiques pour l'utilisateur) et *de facto* il y a même identification presque "inconsciente" par l'ordinateur lui-même, via notre navigateur (Chrome par exemple), qui garde en mémoire non seulement nos références d'instruments de paiement mais aussi un nombre insoupçonné de clés de connexion sécurisée à tous les sites marchands ou autres que nous visitons à longueur de journée.

En regard, l'authentification mise en place par France Connect est moins une clé qu'un trousseau de 3 clés, puisqu'elle agrège l'identification délivrée par les sites des impôts (ce qui peut effrayer), de la poste (peu performant) et de la sécurité sociale (Ameli, notoirement redouté par les usagers pour sa piètre qualité). Il est peu probable que les

---

[50] Malgré tous les changements intervenus depuis lors dans le statut et la mobilité des personnes, les articles 102 à 104 du Code civil n'ont pas changé d'un mot depuis le Consulat !

[51] Voir : https://www.ouest-france.fr/sante/securite-sociale/securite-sociale-2-6-millions-de-cartes-vitale-en-trop-sont-en-circulation-en-france-6736982.

[52] Et pas seulement en 2005, année où fut pour la première fois mise en évidence l'une de ces failles : https://www.zdnet.fr/actualites/la-securite-de-la-carte-vitale-prise-en-defaut-39264579.htm.

[53] *Cf.* https://www.senat.fr/rap/r07-445-2/r07-445-217.html et https://www.rtl.fr/actu/politique/les-infos-de-22h-fraudes-sociales-les-pistes-d-un-rapport-parlementaire-pour-lutter-contre-7798273687.

Français, quand ils n'y sont pas contraints, se servent de cette solution étroitement nationale qui ne les dote pas d'une véritable "identité numérique" ouverte sur le cyberespace.

Au demeurant, derrière les déclarations politiques autour de la protection des données du consommateur européen par le RGPD, on a de multiples raisons[54] de penser que ce fleuron juridique ne gêne guère, et en réalité favorise, les ambitions des GAFAM, de Google en tête, comme l'a rappelé le PDG de Snapchat lui-même.[55] Faut-il même s'en étonner? Toujours, derrière les déclarations, les faits parlent d'eux-mêmes: le choix des portiques américains Cisco par la région PACA pour son test de reconnaissance faciale ne s'imposait pas, au-delà des réserves sur la technologie elle-même. Avec le stress des événements que nous connaissons, les rares scrupules disparaissent aisément: comme le dit crûment le premier quotidien économique français, "*La souveraineté numérique attendra*".[56]

Quoi qu'il en soit, toutes ces logiques exposent les données des utilisateurs pris individuellement à un certain nombre de risques (pillage, piratage, corruption) et de servitudes (surveillance, marketing intempestif…), et notre nation collectivement à une condition numérique qui tient à la fois de la mise en cage et de la mise à nu : en gros, c'est le sort d'une bête au zoo.

L'identité biométrique (pointée par la CNIL) et le projet *Alicem*, dont le Secrétaire d'État au Numérique justifiait l'expérimentation en octobre dernier[57] sous l'habituelle garantie – "pour que nos industriels progressent", il le faut (ce qui ne saurait être une fin en soi). Certes, une forme d'identité biométrique rendrait plus de services en ligne qu'une Carte nationale d'identité à la française, mais elle est surtout utilisée (quelle que soit la pudeur habituelle qui amène à préciser que sa mise en œuvre est une expérience menée avec l'avis de la CNIL, sur la base du volontariat, etc.) par les machines des espaces privés sensibles ou de l'espace publique pour une collecte massive de données qui finiront inéluctablement chez les mieux à même de les gérer, voire de les intercepter, puis de les exploiter: les géants du Net. Il faut ajouter deux faiblesses : le vol de profil (il y en aura) qui sera difficilement réversible et un taux de "faux positifs" qui peut laisser perplexe.

Un système à la fois adapté au monde numérique et tourné vers la protection des données des utilisateurs et le confort d'utilisation devrait s'apparenter davantage à un protocole informatique internationalement interopérable qu'à une application développée par un gouvernement national ou par une entreprise particulière…

Il faudrait tenir compte de la réalité: aujourd'hui, notre identité numérique est (comme celle de nos téléphones !) la somme des traces que nous laissons. Un bon "agglomérateur" pourrait être la somme de toutes ces identités, mais liées par une ou par

---

[54] Il existe innombrables références en ligne sur ce fait, notamment ici la vue d'un universitaire de Paris-I : https://beabilis.com/2018/06/03/pourquoi-google-tirera-le-meilleur-parti-du-rgpd-tout-simplement-parce-quil-est-bon-et-americain/.

[55] *Cf.*https://www.cbnews.fr/mobile/image-regulation-europeenne-favorise-google-facebook-snapchat-43418.

[56] Voir : https://www.lesechos.fr/idees-debats/cercle/la-souverainete-numerique-attendra-1198579.

[57] *Cf.* https://www.lemonde.fr/economie/article/2019/10/14/cedric-o-experimenter-la-reconnaissance-faciale-est-necessaire-pour-que-nos-industriels-progressent_6015395_3234.html.

des clefs dont nous serions les propriétaires. Une sorte de méta-identité, au cœur de nos réseaux, validée pour chaque utilisateur par l'autorité souveraine dont il dépend.

Une *blockchain* permettrait une forme numérique de l'identité (des citoyens, des entreprises, et pourquoi pas des robots et des machines) qui ne soit pas un copié-collé ou une laborieuse numérisation des cartes d'identité ou du Registre du commerce et des sociétés, qui aille beaucoup plus loin que le trousseau de clés de type "France Connect", qui ne soit pas entachée de ce que l'on peut reprocher à l'identité biométrique et qui aille dans la voie d'une identité garantie et rendue inviolable par la cryptographie. La technologie des "ZP" (*zero proof*) fournirait une voie de mise en œuvre.

L'enjeu des langages

Il convient de revenir avant de terminer sur l'enjeu des langages, déjà abordé, mais vu cette fois sous l'angle stratégique de la souveraineté.

Le problème linguistique, dans sa forme "1.0" est bien connu des militaires.[58] Eux-mêmes reconnaissent volontiers qu'ils ont une "langue" propre, au-delà du jargon technique, même dans leur langue maternelle, alors même que, par le brassage de la conscription et des guerres, les Armées ont si puissamment contribué à forger une langue française commune. Parler la langue de l'autre, sur le théâtre des opérations, ou apprendre à l'autre notre langue (l'École de Guerre dispense ainsi des cours intensifs de français sur les objectifs spécifiques pour les officiers étrangers qui souhaitent suivre une formation continue en France) sont des enjeux évidents.

Le problème linguistique dans sa forme "2.0", disons celui du choix des langues de programmation (et de leurs rapports entre elles, du fait de leurs potentialités, de leurs richesses, de leur interopérabilité) ne doit pas être méconnu dans l'optique des opérations de sécurité ou de défense dans le cyberespace.

Mais au-delà des considérations pratiques, la langue est aussi un facteur de prestige diplomatique. On pourrait presque transposer le *Discours sur l'universalité de la langue française* de Rivarol à la situation du langage Ocaml. Ce qu'écrivait Rivarol en 1784, à savoir que "*le goût qu'on a dans l'Europe pour les Français est inséparable de celui qu'on a pour leur langue*", pourrait amener à voir dans le *globish* un signe de l'*avantage moral* concédé aux USA, si Rivarol ne faisait suivre son analyse historique (la suprématie politique de la France) d'une analyse linguistique (l'ordre logique direct de la construction de la phrase française, opposé aux pièges et surprises des langues à inversion) dont on pourrait bien s'inspirer.

Il faut donc, au-delà de la genèse française (à l'INRIA) d'un langage de programmation stabilisé depuis le début du siècle, souligner les caractéristiques, assez *françaises* d'Ocaml finalement, qui se distingue de la plupart des langages développés dans des milieux académiques par d'excellentes performances, lesquelles profitent avantageusement de la nature fonctionnelle, statiquement et fortement typée du langage.

---

[58] Voir les intéressantes réflexions d'un militaire autrichien (c'est-à-dire d'un pays héritier d'un empire multilinguistique) dans les *Cahiers de la Pensée Mili-Terre*, en 2018: https://www.penseemiliterre.fr/vers-une-formation-linguistique-militaire-_416_1013077.html.

Il faut souligner que ce langage, issu des milieux de recherche, enseigné dans les classes préparatoires à nos grandes écoles scientifiques, n'a pas bénéficié de la puissance publicitaire de certains langages de programmation actuels, et que c'est la raison qui explique qu'il reste relativement peu connu du grand public informatique (ainsi que la plupart des langages fonctionnels). Mais qu'il est cependant solidement implanté dans des niches pour lesquelles les qualités du langage contrebalancent son relatif manque de soutien. Il faudrait donc mesurer le poids humain des francophones dans l'écosystème Ocaml et l'enjeu stratégique qu'il y a pour cette raison à appuyer cet écosystème.

Conclusion : Go !

Sans doute les explications techniques qui ont été données ne permettront pas au néophyte de comprendre en finesse ce qui rend la *blockchain* si intéressante en pratique. Nous souhaitons seulement avoir suscité quelques curiosités. Comme toutes les choses réellement novatrices, cette disruption majeure ne se laisse pas appréhender en quelques pages, et il est facile de faire ce que le roi Édouard VII pensait qu'il aurait fait lui-même s'il avait vu sur son chemin le caillou de 3100 carats qu'était le Cullinan non taillé : donner un coup de pied dedans et passer son chemin.

Le lecteur aura vu que les premiers essais, en France et ailleurs, montrent cependant la puissance de la chose, et sa nature à la fois pratique, défensive et stratégique.

Il reste des défis à relever, que nous n'avons pas éludés.

Alors ? Les chocs nés de la pandémie, et les probables difficultés que nous allons traverser, peuvent provoquer une récession intellectuelle: on ne fait rien, on se replie sur ce qu'on sait faire, sur les solutions éprouvées, sur les prestataires dont on a l'habitude et… on laisse la porte ouverte aux GAFAM. Mais ensuite, parler de la souveraineté n'aura plus guère de sens.[59] D'ores et déjà, un certain nombre de choses difficiles à nier ou à contourner font du cyberespace sinon un territoire américain, du moins une *mare nostrum* des Américains. Les autorités françaises, tétanisées par les menaces objectives que fait régner le *Cloud Act*, par exemple, sont néanmoins dépendantes des plateformes d'Apple ou de Google même pour proposer leurs propres applications. Et en matière de collecte de données, comme on l'a vu, elles sont en concurrence avec des GAFAM auxquels les internautes semblent plus enclins à accorder leur confiance qu'à des autorités qui peinent à se faire reconnaître comme "légitimes". Augmenter le volume de données collectées ne fait qu'amplifier l'appétit et la voracité des GAFAM.

Alors, les crises peuvent favoriser chez les plus visionnaires des prises de conscience conduisant à des révolutions. Adopter des architectures ouvertes et décentralisées en lieu et place des silos et des citadelles serait l'une de ces révolutions.

Devant l'immense armée perse, les Athéniens ne savaient que faire et consultèrent l'oracle de Delphes. La Pythie eut comme à l'accoutumée une réponse stupéfiante : "*réfugiez-vous derrière des murailles de bois*". Thémistocle comprit l'oracle. Le bois est

[59] *Cf.* https://www.forbes.com/sites/darrynpollock/2020/04/30/libra-20-more-of-a-progression-than-a-pivot-says-libra-association-member/.

léger, et aucune muraille ne protège un navire, exposé à tout vent, si ce n'est sa mobilité. Mais, distribuée sur toute la mer (et le cyberespace ressemble bien davantage à la mer immense qu'à la terre ferme) et jusqu'au bout du monde, une flotte vous redonne la liberté dont vos propres murailles peuvent parfois vous priver.