Note numéro 35
novembre 2018

Note du CREOGN

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

LA *BLOCKCHAIN* : UNE TECHNOLOGIE ÉMERGENTE AU POTENTIEL À EXPLORER

Par le lieutenant Jean-Baptiste MUNOZ

La technologie *blockchain,* ou « chaîne de blocs » en français, est devenue un sujet qui agite tant les acteurs numériques que les organes de gouvernance des pouvoirs publics ou privés. Pas un jour sans que la presse spécialisée ou les grands quotidiens n'en parlent, mais bien peu sont à même de comprendre le fonctionnement de cette évolution numérique et son implication pour l'avenir[1].

Blockchain[2] *France* définit la *blockchain* comme une « technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle »[3]. La *blockchain* est une base de données décentralisée. Elle s'oppose aux bases de données centralisées dont les défauts principaux sont de ne pouvoir travailler sans accès au registre unique et de nécessiter des infrastructures initiales coûteuses pour accueillir les serveurs. Conceptuellement parlant, la *blockchain* s'inscrit dans le cadre des logiciels libres et des réseaux pair-à-pair, en tentant d'éluder les acteurs institutionnels classiques.

La mise en place d'une *blockchain* est une prouesse technologique, car ce système décentralisé ne peut fonctionner qu'en résolvant un problème informatique appelé le « problème des généraux byzantins »[4]. Dans ce cas, il s'agit de faire face, d'une part, à l'asynchronisme lié à la décentralisation de la base de données et, d'autre part, de prévenir les malveillances. Ainsi, la *blockchain* du Bitcoin[5] a été la première à mettre en œuvre cette technologie, avec le succès qu'on lui connaît aujourd'hui.

Cette technologie intéresse particulièrement les pouvoirs publics en France qui ne veulent pas rester en marge de son potentiel. C'est pour cela qu'un rapport parlementaire a été présenté aux Chambres le 20 juin 2018[6] dans le cadre de la mission d'information commune sur « les usages des *blockchains* et autres technologies de certification des registres ».

La *blockchain* est une technologie ambitieuse dont les débouchés doivent être bien définis (I), en tenant compte des limites qu'il faudra dépasser pour permettre son expansion (II).

I/ La *blockchain*, une technologie prometteuse bien au-delà des cryptomonnaies

Les thuriféraires de la *blockchain* affirment que cette technologie va jouer un rôle central dans l'existence des gens en se substituant, dans un avenir proche, aux tiers de confiance tels que les banques, les notaires ou encore les compagnies d'assurances.

1ALEXANDRE, Laurent. Blockchain, je n'y comprends rien !, *L'Express L'expansion*, 30 octobre 2018. Disponible sur : https://lexpansion.lexpress.fr/high-tech/blockchain-je-n-y-comprends-rien_2044313.html

2 « Blockchain France accompagne les organisations dans la découverte, l'exploration et le déploiement des technologies blockchain ». Disponible sur : https://blockchainfrance.net/

3 BLOCKCHAIN FRANCE. *Qu'est-ce-que la Blockchain ?* Disponible sur : https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain

4 LAMPORT, Leslie, SHOSTAK, Robert, PEASE, Marshall. « The Byzantine Generals Problem », *ACM Transactions on Programming Languages and Systems*, 4, 3.

5 NAKAMOTO, Satoshi, *Bitcoin a peer-to-peer electronic cash system*, 2008.

6 Rapport au nom de l'office parlementaire d'évaluation des choix scientifiques sur « Les enjeux technologiques des blockchains (chaînes de bloc) », 20 juin 2018. Disponible sur : https://www.senat.fr/rap/r17-584/r17-5841.pdf

A) La recherche d'applications concrètes fondées sur la technologie *blockchain*

Aujourd'hui, les possibilités évoquées en termes d'utilisation de la technologie sont nombreuses, mais rares sont les initiatives arrivées à leur terme. Dans les pays développés, la *blockchain* peut sembler superfétatoire au regard de ce qui est déjà en place. L'impact technologique sera sûrement moins révolutionnaire dans les pays occidentaux où l'État joue un rôle important dans la normalisation et la régulation des échanges et des transactions. Cependant, la *blockchain* pourrait permettre de réduire les coûts de fonctionnement. Il n'est pas anodin que le premier déplacement d'Édouard Philippe à l'étranger après sa nomination à Matignon fut l'Estonie. Ce pays de l'Union européenne a mis en place une administration numérique dont l'infrastructure cryptographique est similaire au fonctionnement d'une *blockchain*. Chaque Estonien dispose d'une carte d'identité électronique lui permettant d'accéder à 2 000 services et faisant économiser à l'État 2 % de son PIB par an[7].

Les universités et les grandes écoles pourraient également se servir de la *blockchain* pour la mise en place d'un registre des publications académiques, des diplômes délivrés, etc. L'administration fiscale pourrait trouver intérêt à utiliser cette technologie pour réduire les coûts liés au prélèvement de l'impôt. En ce qui concerne la Sécurité Sociale, la *blockchain* permettrait d'authentifier les soins et services reçus par les patients.

Dans les pays les moins avancés, la fiabilité et la transparence de la *blockchain* garantiraient des transactions diverses hors domaine financier. Au Ghana, l'organisation *Bitland* utilise la *blockchain* pour établir un cadastre officiel[8]. D'autres applications sont appelées à se développer progressivement pour limiter les litiges. La *blockchain* pourra certifier les processus électoraux et limiter les contestations et autres émeutes post-scrutin. À cet égard, les premières expériences de vote électronique sont testées en Virginie.

B) Les débouchés de la *blockchain* pour le monde entrepreneurial et l'essor des « *smart contracts* »

Les grands groupes privés cherchent actuellement à trouver des utilisations commerciales à la technologie *blockchain* pour améliorer leurs processus. L'entreprise Carrefour a, par exemple, instauré un système de *blockchain* pour tracer sa filière de volailles afin d'en garantir la certification et l'origine[9].

La *blockchain* a la faculté de gérer les « contrats intelligents ». Les « *smart contracts »* ne sont pas des contrats juridiques. Il s'agit en l'espèce d'une série de lignes de code qui va déclencher automatiquement une action. On parle ici « de coupler la dimension transactionnelle au monde physique, ce qu'on appelle l'Internet de la valeur »[10]. Cet item intéresse déjà le secteur de l'assurance à plusieurs niveaux, tant pour la résiliation de contrats que pour automatiser des procédures d'indemnisation afin de rembourser les voyageurs en cas de retard d'un avion par exemple. La fédération française de l'assurance est déjà satisfaite des premiers résultats obtenus. Elle continue ses recherches pour que l'utilisation de la *blockchain* soit généralisée, permettant ainsi de réduire les coûts tout en assurant un haut niveau de sécurité[11].

Les projets concrets issus de la technologie *blockchain* restent donc encore très limités mais on assiste déjà à des expérimentations prometteuses pour l'avenir. Il ne faut pas pour autant en oublier les risques induits, qui seront à atténuer pour envisager la démocratisation de ses applications.

II/ Les risques liés à l'utilisation de la technologie *blockchain*

Trois types de risques majeurs semblent émerger de l'utilisation des « chaînes de bloc » : la menace d'agression du système et de son fonctionnement en dépit de sa solidité intrinsèque, l'utilisation par les

7 CHERIF, Anaïs, MANIÈRE, Pierre. L'Estonie, royaume du tout-numérique, *La Tribune*, 5 avril 2018. Disponible sur : https://www.latribune.fr/technos-medias/internet/l-estonie-royaume-du-tout-numerique-774138.html

8 ABERKANE, Idriss J. Blockchain, le bond en avant africain, *Le Point,* 27 mars 2018. Disponible sur : http://afrique.lepoint.fr/actualites/idriss-aberkane-blockchain-le-bond-en-avant-africain-27-03-2018-2205749_2365.php

9 DENUIT, Delphine, BOUSSARD, Agathe. Carrefour permet de tracer ses poulets fermiers grâce à la blockchain, *Le Parisien*, 6 mars 2018. Disponible sur : http://www.leparisien.fr/economie/carrefour-permet-de-tracer-ses-poulets-fermiers-grace-a-la-blockchain-06-03-2018-7593969.php

10 MAREUGE, Céline. Les enjeux des blockchains, *France Stratégie*, 21 juin 2018. Disponible sur : http://www.strategie.gouv.fr/publications/enjeux-blockchains

11 Expérimentation d'une Blockchain inter-assureurs autour de l'échange de données sécurisées, *Fédération française de l'assurance*, 9 novembre 2017. Disponible sur : https://www.ffa-assurance.fr/content/experimentation-une-blockchain-inter-assureurs-autour-de-echange-de-donnees-securisees-0

délinquants de cette technologie et l'impact écologique lié à la consommation énergétique importante pour faire fonctionner la *blockchain*.

A) Les attaques contre les *blockchains* et l'utilisation de cryptomonnaies dans le cadre d'activités illicites

1. Les attaques contre le système

La spécificité de cette technologie est justement la sécurité, car il est très difficile d'attaquer une *blockchain*. Un registre distribué sur plusieurs nœuds partout dans le monde au même moment est bien moins vulnérable qu'un registre centralisé sur un serveur unique. Cependant, comme dans tout système, il existe des failles et des attaques ont déjà eu lieu. La *blockchain* du Bitcoin a été attaquée le 15 août 2010 et il a fallu près de neuf heures pour que le « bug » créé soit corrigé. Un autre type d'attaque possible de la *blockchain* résiderait dans une « attaque 51 % », c'est-à-dire que l'assaillant prendrait le contrôle de la majorité de la puissance de calcul nécessaire au fonctionnement de la *blockchain* pour imposer ses décisions. Cette hypothèse reste peu probable, car l'assaillant devrait déployer des ressources si importantes qu'il ne tirerait pas de bénéfices de son attaque.

2. L'exploitation par les criminels

Les délinquants tirent déjà profit de son utilisation en se servant des cryptomonnaies pour leurs activités illégales. La *blockchain* séduit le crime organisé, d'une part, en raison de la fiabilité des échanges et, d'autre part, de la pseudonymisation des transactions. Les cryptomonnaies permettent d'acheter des produits et services illégaux comme les drogues, les logiciels piratés, les armes, les médicaments contrefaits, ou encore des contenus pédopornographiques. Un tiers des utilisateurs de Bitcoin l'utiliserait pour ce genre d'activités illégales, qui représenteraient la moitié de toutes les transactions en Bitcoin[12]. On parle dans ce cas du « Paypal du *dark web* ».

Toutefois, il serait erroné de penser que le*s cryptomonnaies* seraient un problème majeur. Elles représentent une infime partie des revenus financiers du crime organisé, et l'argent liquide reste en effet bien plus complexe à tracer. Dans le cas des cryptomonnaies, tout est archivé, c'est même la fonction première de cette technologie. On peut identifier et tracer toutes les transactions d'un individu, dès lors que l'on trouve sa clé de cryptage lors des perquisitions. C'est un avantage considérable pour les magistrats, dans la mesure où elle constitue une preuve numérique, car la *blockchain* est publique, certifiée et non falsifiable. Les magistrats français n'ont d'ailleurs pas hésité à reconnaître le lien entre une infraction sur Internet et le possesseur de la clef qui a commis le méfait. Le coût de cet investissement en compétences et en ressources est important pour les services de la gendarmerie nationale. Le centre de lutte contre les criminalités numériques (C3N) investit annuellement plusieurs centaines de milliers d'euros dans des outils pour lutter contre cette nouvelle forme de délinquance.

3. Les escroqueries aux levées de fonds

Enfin, comme toute technologie émergente, beaucoup de personnes veulent participer à ce nouveau phénomène qui semble très rentable lorsque l'on s'attarde sur les fluctuations des cours du Bitcoin. Une des applications phares des *blockchain* réside dans l'Initial Coin Offering (ICO), des levées de fonds sur le schéma « crowdfunding ». En 2018, cela représentait près de 8 milliards d'euros. Les escroqueries et arnaques sont nombreuses[13]. On assiste régulièrement à la disparition des sociétés après la levée de fonds. Google, Facebook et Twitter ont supprimé en mars 2018 la possibilité pour les ICO, et les cryptomonnaies de manière générale, de faire de la publicité sur leurs réseaux sociaux.

12 FOLEY, Sean, KARLSEN, Jonathan, PUTNINS, Talis. « Sex, drugs & bitcoin: How much illegal activity is financed through cyptocurrencies », *University of Sydney*, dernière mise à jour du 23 octobre 2018.

13 DELUZARCHE, Céline. Cryptomonnaie : l'épave emplie d'or cachait une gigantesque arnaque, *Futura sciences*, 24 août 2018. Disponible sur : https://www.futura-sciences.com/sciences/actualites/histoire-cryptomonnaie-epave-emplie-or-cachait-gigantesque-arnaque-72521/

B) La consommation énergétique toujours croissante

La « preuve de travail » est le consensus algorithmique principalement employé pour faire fonctionner les *blockchain* qui a pour particularité de demander une puissance de calcul exponentielle. Il est difficile d'évaluer avec exactitude la consommation électrique d'une *blockchain*, cependant plusieurs méthodes d'estimation ont été proposées. Certaines laissent supposer qu'il faudrait en moyenne sept réacteurs nucléaires pour fournir l'électricité suffisante à alimenter les *blockchains* actuellement basées sur la « preuve de travail »[14].

Les opérateurs les plus actifs des *blockchains* vont chercher à travers le monde à se fournir en électricité à bas coût, notamment produite par les centrales à charbon, avec un impact environnemental considérable. La Chine accueille de plus en plus de serveurs alors que son empreinte carbone est déjà la plus élevée au monde. Aux États-Unis, la ville de Plattsburg a interdit l'installation de nouvelles installations de calcul en février 2018 pour combattre l'augmentation du prix de l'électricité pour ses citoyens[15].

Pour les spécialistes ayant été interrogés dans le cadre du rapport parlementaire sur « les enjeux technologiques des blockchains », ce problème énergétique vient du consensus dit de la « preuve de travail ». Pour pérenniser l'utilisation de cette technologie *blockchain*, il est impératif de solutionner cette question en allant vers des consensus moins énergivores. Aujourd'hui, des évolutions sont déjà en cours, l'Ethereum, la *blockchain* la plus importante après celle du Bitcoin, étant par exemple en train d'effectuer la bascule vers un consensus plus respectueux de l'environnement.

La technologie *blockchain* est sans aucun doute une révolution numérique dont les applications ne sont pas encore assez matures pour être utilisées par la population. On ne sait pas si elle viendra supplanter les systèmes déjà existants dans les pays développés. Une chose est sûre, cependant, la *blockchain* trouve déjà son chemin dans les pays les moins avancés afin de garantir sécurité et transparence là où les institutions ne sont pas jugées assez fiables.

Le gouvernement français a décidé de ne pas rester à la marge de cette évolution technologique. Les pouvoirs publics en France sont en train de fixer petit à petit un cadre légal autour de la *blockchain* afin de sécuriser les utilisateurs, tant contre les fraudes que pour assurer la protection des données personnelles des utilisateurs.

Les grands acteurs du numérique tels que les GAFAs restent sceptiques tout en expérimentant dans leurs réseaux propres cette technologie. Cependant, le fonctionnement décentralisé de la *blockchain* pourrait aussi devenir le tombeau de géants comme Facebook, les utilisateurs pouvant à travers la gouvernance décentralisée se passer des GAFAs pour échanger des données en toute transparence et de manière sécurisée.

Avant même d'avoir impacté nos vies, la *blockchain* sera peut-être tombée aux oubliettes, supplantée par des systèmes plus efficaces permettant de résoudre le problème de la « scalabilité » de la *blockchain*, c'est-à-dire sa capacité à monter en charge et d'augmenter le nombre de transactions traitées tous les jours. Des technologies de registres distribués alternatives aux *blockchains* sont déjà en cours de développement dans les laboratoires de recherche. Ainsi, les « *Directed Acyclic Graphs* » (DAG)[16], « *blockchain* nouvelle génération », offrent un fonctionnement plus rapide, plus efficace et moins cher. À l'heure actuelle, cela reste expérimental mais pourrait constituer une solution décentralisée à la gestion des objets connectés qui se multiplient.

14 OPECST, données du 2 juin 2018.
15 « Is Bitcoin a Waste of Electricity, or Something Worse ? », *The New York Times*, 28 février 2018. Disponible sur : https://www.nytimes.com/2018/02/28/business/economy/bitcoin-electricity-productivity.html
16 LEE, Sherman. « Explaining Directed Acylic Graph (DAG), The Real Blockchain 3.0 », *Forbes*, 22 janvier 2018. Disponible sur : https://www.forbes.com/sites/shermanlee/2018/01/22/explaining-directed-acylic-graph-dag-the-real-blockchain-3-0/#3ed31a7180bc