

La *blockchain* au service de l'action publique

Par Malo CARTON

Ingénieur des mines, Agence des participations de l'État (APE)

et Pierre JÉRÉMIE

Ingénieur des mines, chef du service de prévention des risques et des nuisances, direction régionale et interdépartementale de l'environnement et de l'énergie (DRIEE) d'Île-de-France

La technologie *blockchain* offre la possibilité de construire des registres décentralisés et de partager la confiance entre opérateurs dans la validité de ces registres. La décentralisation des bases de données sous-jacentes à une *blockchain* est consubstantielle à cette technologie. Dans le cas de l'action publique, une telle décentralisation constitue un changement de paradigme pour l'organisation habituelle de données publiques jusque-là stockées par un ou plusieurs opérateurs publics étroitement surveillés. Nous présenterons ici deux champs d'action publique pour lesquels la mise en œuvre de solutions utilisant cette technologie est actuellement à l'étude : la mise en place d'une nouvelle chaîne de titres pour assurer une circulation des titres financiers plus fluide, mais aussi plus aisément contrôlable, et les possibilités offertes par la *blockchain* pour l'enregistrement des droits et des servitudes sur les sols au service d'une meilleure information des acquéreurs.

Introduction

Alors qu'à l'origine, par le biais de la communauté d'utilisateurs du protocole bitcoin, la technologie *blockchain* s'est construite par opposition au modèle centralisé standard prévalant dans l'action gouvernementale, selon une conception « libertarienne » des rapports économiques et sociaux, les promesses de la technologie ont amené les gouvernements de plusieurs pays de l'OCDE (dont la France), à considérer avec attention les applications potentielles d'une telle technologie. Nous nous proposons, dans cet article, de présenter quelques caractéristiques de la *blockchain* qui peuvent justifier l'intérêt qu'a suscité cette technologie dans le cadre de l'action publique. Deux exemples seront plus amplement détaillés, l'un étant tiré de l'actualité législative récente, et l'autre plus exploratoire afin de mettre en avant quelques applications types qui sont attendues de cette technologie dans le cadre de l'action publique.

Les principales caractéristiques de la *blockchain* présentant un intérêt pour l'action publique

Une *blockchain* est avant tout une méthode d'implémentation d'un registre distribué (c'est-à-dire réparti entre les différents nœuds d'un réseau) et protégé contre des modifications des données enregistrées, y compris de la part de ceux qui la mettent en œuvre.

Schématiquement, deux types d'opérateur sont présents

sur une *blockchain* :

- d'une part, des utilisateurs qui souhaitent voir stockées des informations et/ou consulter des informations qui le sont déjà ;
- d'autre part, des « mineurs » : ce sont des utilisateurs qui mettent à la disposition du réseau, souvent contre une rémunération déterminée dans le protocole, leurs capacités de calcul dans le cadre d'une preuve de calcul (*proof of work*) pour assurer la validation des informations et la gestion décentralisée du registre.

Au-delà des différentes technologies envisageables pour mettre en œuvre une *blockchain*, il convient tout d'abord d'examiner (dans le cadre de cet article) les propriétés fondamentales des *blockchains* qui peuvent s'avérer intéressantes pour l'action publique :

- leur caractère distribué permet de répartir la charge de la mise en œuvre de ces registres entre un grand nombre d'utilisateurs, y compris hors État (collectivités, opérateurs agréés, etc.) ;
- leur construction rend les *blockchains* résilientes à des attaques : en pratique, les données stockées sont gravées dans le marbre, définitivement, et ne peuvent être altérées (y compris par les opérateurs du registre), une fois qu'elles ont été validées⁽¹⁾ ;

(1) Cela tant que des évolutions techniques ne permettent pas de casser en un temps relativement court les chiffements employés ou la « preuve de travail » de la *blockchain*.

- elles permettent de construire structurellement un consensus sur la validité des données enregistrées et sur leur chronologie ;
- n'importe quel nœud d'une *blockchain* peut aisément vérifier si une donnée figure ou non dans la base.

La décentralisation des bases de données sous-jacentes à une *blockchain* est consubstantielle à cette technologie. Dans le cas de l'action publique, une telle décentralisation peut conduire à modifier en profondeur l'organisation habituelle de données publiques qui jusqu'ici étaient stockées par un ou plusieurs opérateurs publics étroitement surveillés. Cette décentralisation va de pair avec la vérification par n'importe quel nœud (c'est-à-dire par n'importe quel utilisateur) des données qui figurent dans la *blockchain*. Suivant les décisions de politique publique souhaitées, on peut imaginer, grâce à cette technologie, d'offrir aux citoyens la possibilité d'accéder à un haut niveau de transparence, tout en leur permettant de participer activement au système, en en représentant des nœuds stockant une partie des données. Cela pose nécessairement la question du champ d'ouverture de ces données : souhaite-t-on par exemple les ouvrir à tous les citoyens, dans un souci de transparence (à l'instar, par exemple, du cadastre, ou des données sur l'état de l'environnement⁽²⁾) ?

Par ailleurs, pour conforter la résilience de la *blockchain* (inaltérabilité des données inscrites) procédant du protocole de validation des blocs, et notamment de la force du consensus, la question des mineurs est cruciale, dans le cas d'une *blockchain* destinée à l'action publique. Là encore, on peut imaginer mobiliser une technologie *blockchain* comme moyen permettant de donner du pouvoir aux citoyens, en leur conférant un pouvoir de vérification renforçant d'autant la confiance que peuvent susciter les données concernées.

En raison de ses principales caractéristiques, la *blockchain* apparaît dès lors être un moyen de refonder certains modes de fonctionnement en conférant aux citoyens (ou à un sous-ensemble de citoyens) un pouvoir aujourd'hui réservé ou fortement interfacé par la puissance publique. Dans un contexte de défiance vis-à-vis de certaines institutions de contrôle, les promesses d'une telle technologie plus consensuelle et horizontale peuvent être intéressantes. Plus prosaïquement, on peut aussi considérer que, dans certains cas, la mise en place par l'État d'un tel système pourrait conduire à une organisation plus efficace de systèmes aujourd'hui sujets à des rentes de situation ou à des inefficiences technologiques (voir les exemples des titres financiers, ci-après).

Blockchain et action publique : deux déclinaisons concrètes

De la monnaie électronique à la construction d'une nouvelle chaîne de titres au service du financement de l'économie et d'un meilleur suivi des transactions

Comme évoqué plus haut, la technologie de la *blockchain* permet d'implémenter de manière décentralisée un registre résistant à des attaques, enregistrant des données

de manière définitive et partagée, avec un consensus des utilisateurs sur le contenu de ce registre. Un grand nombre de métiers requièrent des registres inaltérables, consensuels et publics. Ils étaient, de ce fait, irréalisables – avant l'irruption du numérique – en l'absence d'une autorité centralisée certifiant l'inaltérabilité et venant apporter sa garantie valant consensus. Ils étaient donc en général confiés soit aux États, soit à des opérateurs privés de grande taille (le plus souvent soumis à un fort contrôle public).

L'exemple d'utilisation de la *blockchain* le plus connu du grand public est le protocole bitcoin, pour lequel le registre implémenté est un registre de transactions d'une monnaie virtuelle grâce auquel la *blockchain* permet de décentraliser la confiance dans la régularité des transactions et la validité de la monnaie présentée (un rôle confié de tout temps, pour les monnaies fiduciaires ou métalliques, à l'État ou à une banque centrale disposant d'un monopole, s'érigeant ainsi en « tiers de confiance » ultime).

Parmi les nombreuses applications attendues de la « chaîne de blocs », l'évolution des modalités de représentation et de circulation des titres financiers suscite l'attention du secteur financier : des financements importants sont d'ores et déjà mobilisés, en France, mais surtout dans les pays anglo-saxons.

Si le droit applicable aux titres financiers – et le fonctionnement des infrastructures et acteurs associés (dépositaire central de titres, teneurs de compte, etc.) – est longtemps resté discret, sinon inconnu, c'est que ce domaine cantonné à un débat d'experts, entre juristes et « titrards » des établissements financiers, était perçu comme moins stratégique que celui de la négociation (la corbeille) ou de l'orchestration des opérations sur le capital.

Toutefois, en l'absence d'une chaîne robuste du titre, le transfert de propriété des titres, contrepartie juridique du règlement d'une transaction financière en espèces, ne peut être garanti. C'est dès lors le fonctionnement des marchés financiers qui est remis en cause dans son fondement même. Tant pour des raisons opérationnelles que pour des raisons de supervision des acteurs, les participants de la chaîne du titre ont été historiquement centralisés, ou au moins organisés en « arbres », chaque nœud représentant un teneur de compte, et le nœud de plus haut niveau représentant le dépositaire central. Pour une transaction donnant lieu à un transfert entre deux participants qui ne sont pas les clients d'un même teneur de compte, l'opération doit être validée par chacun des deux teneurs de compte, qui doivent eux-mêmes en référer au dépositaire central responsable de l'intégrité de l'ensemble des titres en circulation.

Cette logique est fondamentalement antagonique avec la logique du protocole *blockchain*. Les transactions ne sont pas validées par consensus décentralisé entre tous les acteurs de marché, mais par un seul intermédiaire, centralisé

(2) Convention d'Arhus, directive INSPIRE.

et fortement régulé (compte tenu du pouvoir exorbitant qui lui a été ainsi conféré). Incidemment, il convient de noter que cette organisation peut rapidement s'avérer problématique du point de vue économique, en raison de la présence d'un acteur en situation de monopole de fait qui peut être tenté de prélever une rente sur les utilisateurs. Historiquement, la solution qui avait été trouvée consistait à faire participer les principaux acteurs financiers au capital du dépositaire central (c'était le cas en France, avec la Sicovam, détenue à l'origine principalement par des banques françaises), ce qui permettait de limiter le risque d'un comportement de rentier de la part du dépositaire.

Dans ce contexte, que peut apporter la chaîne de blocs au fonctionnement de la chaîne du titre ?

Tout d'abord, elle permet d'éviter une structure arborescente, qui ferait reposer l'intégrité de la chaîne sur un seul maillon, le nœud de plus haut niveau, qui devrait être très fortement régulé, ce qui conduirait en retour à un possible comportement de rentier de la part de cet acteur, et ce, au détriment de l'ensemble du système (coûts excessifs, inefficiences, etc.).

Par ailleurs, dans le cas des titres non cotés, la mise en place d'une solution chaîne de blocs représenterait un important saut technologique comparable à la dématérialisation des titres cotés intervenue en France en 1984. Cela serait de nature à favoriser l'écosystème du financement désintermédié, en renforçant la robustesse et la vérifiabilité des transactions portant sur des titres non cotés.

Enfin, en consignnant dans un registre décentralisé l'ensemble des transactions sur les titres, et non pas en donnant une image statique des propriétaires des titres à un instant donné, le niveau d'information auquel peuvent avoir accès d'éventuels contrôleurs (administration fiscale, Autorité des marchés financiers) serait substantiellement renforcé, leur permettant à tout instant de disposer d'une vision du portefeuille des acteurs du marché et d'en reconstruire l'historique.

Dans ce contexte, des avancées ont été annoncées par le précédent gouvernement pour promouvoir le développement de cette nouvelle technologie.

Deux annonces successives ont été faites : tout d'abord, l'annonce d'une expérimentation pour l'utilisation d'une chaîne de blocs pour les « minibons » (ordonnance du 28 avril 2016 relative aux bons de caisse), puis l'annonce d'un cadre réglementaire pour l'utilisation d'une chaîne de blocs pour les titres financiers non cotés dans le cadre de la loi relative à la Transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite « loi Sapin 2 ».

Les minibons sont des instruments de financement, qui, sans être des titres de créance ou des contrats de prêt, matérialisent une reconnaissance de dette sur une entreprise. Il s'agit d'une remise au goût du jour d'un vieil instrument de financement, le bon de caisse, dans le cadre du financement participatif.

L'ordonnance précitée, prise en application de la loi « Macron », a permis de réformer le cadre réglementaire

des bons de caisse afin de créer les minibons. Durant les travaux préparatoires de l'ordonnance, il a été jugé opportun de réserver au niveau législatif la possibilité de mettre en place, par décret pris en Conseil d'État, un mécanisme du type chaîne de blocs pour la représentation et la mise en circulation de ces nouveaux instruments de financement.

Cela a ainsi permis d'inscrire au niveau législatif, dès le début de l'année 2016, la première définition d'une chaîne de blocs en droit français au sein du Code monétaire et financier (et, à la connaissance des auteurs, en droit européen) :

« Art. L. 223-12 – Sans préjudice des dispositions de l'article L. 223-4, l'émission et la cession de minibons peuvent également être inscrites dans un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations dans des conditions, notamment de sécurité, définies par décret en Conseil d'État. »

La solution retenue présente l'avantage de l'optionnalité, tout en réservant de la place à l'expérimentation de ce nouveau mode de fonctionnement des activités de post-marché, si les circonstances sont réunies.

Cette solution a été possible dans le cadre de cette ordonnance, car, contrairement à l'univers des titres financiers (surtout ceux qui sont cotés), le régime juridique applicable aux bons de caisse était quasiment inexistant et ne procédait d'aucun texte européen. L'espace était donc libre pour mettre en place les premiers jalons d'un cadre nouveau, qu'il conviendra de préciser lors de l'adoption du décret prévu à l'article L. 223-12. Toutes choses égales par ailleurs, on peut rapprocher cette situation de celle du développement des télécommunications mobiles dans les pays en développement : il est parfois plus simple de passer tout de suite au meilleur niveau de l'état de la technique lorsque l'on part d'une « feuille blanche ».

S'agissant de la loi Sapin 2, une habilitation à procéder par voie d'ordonnance a été prévue pour définir un cadre réglementaire en vue de la mise en place d'une solution de type *blockchain* pour des titres non cotés. Une consultation publique est en cours pour déterminer les contours de la régulation qui pourrait ainsi être mise en place. La France sera alors l'un des premiers pays en Europe à se doter d'un tel cadre réglementaire, qui pourra éventuellement être étendu au cadre européen, notamment pour les titres cotés⁽³⁾.

Dans les deux cas, en partant des avantages du cadre existant et des contraintes juridiques applicables, l'approche suivie à ce jour en France pour l'application de la technologie chaîne de blocs à la chaîne du titre est à la fois graduelle et hybride.

Graduelle, elle l'est pour initier les expérimentations dans des cas d'usages naissants (minibons) ou en complément d'un cadre existant peu satisfaisant (titres non cotés).

(3) http://www.tresor.economie.gouv.fr/16101_consultation-publique-ordonnance-blockchain-applicable-a-certains-titres-financiers

Hybride, elle l'est lorsqu'il s'agit de ne pas basculer l'ensemble du cadre de représentation et de circulation des titres dans la chaîne de blocs, pour chercher, au contraire, à appuyer le développement de la chaîne de blocs, notamment au service de l'enregistrement des transactions, en misant sur la force juridique de la représentation des comptes-titres. La chaîne de blocs peut alors devenir un nouveau mode, davantage décentralisé, d'administration d'un compte-titre centralisé, qui continuerait à avoir force juridique pour ce qui est de la propriété des titres.

Blockchain et livre foncier : vers l'intégration dans le système des titres de propriété à l'attention des acquéreurs d'informations sur les risques et les nuisances

Une autre mission particulièrement régaliennne des États est l'implémentation du cadastre, d'une part (au sens de registre public des parcelles existantes par entité administrative), et d'un registre des propriétés foncières, d'autre part, certifiant la propriété de ces parcelles. Ce travail, dont on trouve des traces depuis la plus haute antiquité, remplit plusieurs fonctions : d'une part, apporter la connaissance des assiettes fiscales pour les impôts calculés sur une base foncière, dont la publicité et l'inaltérabilité sont des garanties démocratiques acquises lors de la Révolution française et, d'autre part, apporter la garantie publique aux titres de propriété foncière.

Il est parfaitement envisageable, sur un plan technique, de numériser ces deux documents dans un registre de type *blockchain*, répondant, par construction, aux impératifs de publicité, d'inaltérabilité et de consensus requis. Plus concrètement, les autorités publiques ayant pouvoir sur le cadastre ou assurant la validité légale et la certification des changements de propriété foncière (les notaires, notamment) pourraient être les « mineurs » d'une *blockchain* rendant accessibles à tous les données de tel ou tel propriétaire. La plasticité d'un tel registre permettrait d'ailleurs d'intégrer dans un registre décentralisé unique d'autres types de données, notamment, pour les différentes parcelles, les informations relatives aux prescriptions d'urbanisme applicables et toute information relative à ces parcelles.

Il devient ainsi imaginable de construire un système décentralisé d'enregistrement des mutations foncières dans lequel les transactions immobilières seraient saisies par des officiers ministériels (les notaires, par exemple), ce qui permettrait à l'administration de disposer également, à des fins fiscales, de l'inventaire des propriétés parcellaires, soit l'ensemble des fonctions actuellement remplies par le livre foncier. En pareil cas, outre ces transactions, le registre décentralisé de la chaîne de blocs permettrait également de saisir des « transactions spéciales » qui viendraient simplement « rattacher » aux parcelles les prescriptions applicables ou les données environnementales afférentes, dans une base de données décentralisée. Ainsi, on pourrait imaginer qu'un service chargé de l'urbanisme puisse disposer des droits lui permettant de rattacher à une parcelle les prescriptions prévues dans le plan

local d'urbanisme et dans les plans de prévention des risques ou les servitudes d'utilité publique applicables, qu'un service chargé du suivi des pollutions existantes des sols puisse saisir les informations relatives aux secteurs d'information sur les sols issus de la loi ALUR (art. 173) en en assurant une consultation facilitée et une mise à disposition « en une fois » pour d'éventuels acquéreurs. En automatisant la mise à disposition des données environnementales et des règlements d'urbanisme attachés à une parcelle, un tel dispositif permettra non seulement de réaliser des gains importants d'efficacité en abolissant les consultations systématiques des services en charge de ces questions lors des mutations foncières, en fluidifiant les transactions immobilières et en facilitant l'identification tant de situations problématiques que les secteurs les mieux appropriés à des projets d'aménagements. La construction du dossier préalable à une acquisition (la liasse, fort épaisse, qu'il convient de parapher devant notaire) ne prendrait plus que le temps d'un clic pour retrouver les informations pertinentes sur le bien considéré.

Le rôle de l'État passerait de celui d'autorité de certification d'un registre centralisé des données à un rôle de garant de l'intégrité du protocole et des moyens de chiffrement mis en œuvre, ce qui suppose un renversement d'optique de première importance pour ces missions très régaliennes. La mise en œuvre de cadastres numériques décentralisés basés sur la chaîne de blocs pourrait cependant trouver une application dans des pays en développement ne disposant pas de registre centralisé et dans lesquels la garantie des droits de propriété représente un enjeu fort pour le développement économique. Une expérimentation en la matière est le projet Bitland, qui vise à déployer un tel dispositif au Ghana⁽⁴⁾. Là encore, comme dans le cas des minibons, il est parfois plus simple d'aller directement à la pointe de la technologie, quand on part d'une feuille blanche.

Conclusion

À l'heure où émerge la chaîne de blocs, celle-ci peut apparaître comme une opportunité de restaurer une horizontalité entre utilisateurs du réseau, en en faisant simultanément des prestataires et des utilisateurs de services tant numériques que réels, dans une approche pair-à-pair : l'action publique a tout à gagner à se saisir de cette possibilité pour assurer le maintien des registres d'opérations ou de propriété au service du contrôle, dans des domaines aussi distincts que le suivi des droits et servitudes foncières ou la maîtrise de la chaîne de titres. Cette évolution permettra non seulement une meilleure fluidité des échanges, mais également un contrôle plus aisé des opérations, conduisant à un fonctionnement efficient des marchés. Cette évolution supposera toutefois une évolution substantielle de la relation contrôleur/contrôlé, en plaçant les contrôlés en capacité d'assurer une partie du contrôle de la correction des saisies dans la chaîne.

(4) <http://bitlandglobal.com/>