À quoi peut bien servir la chaîne de blocs ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 28 août 2016

http://www.bortzmeyer.org/a-quoi-sert-blockchain.html

Tous les jours, plusieurs articles apparaissent dans les médias pour expliquer que la chaîne de blocs ("*blockchain*" dans la langue de Satoshi Nakamoto) va résoudre encore un nouveau problème. Pour le non-spécialiste, il n'est pas évident de faire la part du réel et du fantasme dans toutes ces applications de la chaîne de blocs. C'est en pensant à ce non-spécialiste que j'ai écrit cet article : peu ou pas de technique, juste une exploration des choses où la chaîne de blocs est vraiment utile, par rapport à celles où elle n'a pas d'intérêt.

D'abord, je vais me permettre un court paragraphe rappelant ce qu'est la chaîne de blocs : il s'agit d'une base de données ordonnée (les blocs contiennent des transactions, opérations d'écriture dans la chaîne, qui sont dans un ordre précis), répartie sur un réseau (typiquement Internet), et qui n'a pas de gérant unique. Chaque machine, chaque **nœud**, porte toute la chaîne et détruire celle-ci nécessiterait donc de détruire des dizaines de milliers de machines, gérées par des gens différents. La chaîne de blocs est **publique** : tout le monde peut créer un nœud du jour au lendemain, qui va automatiquement télécharger et vérifier la chaîne, avec toutes les données qu'elle contient. Tout le monde peut y écrire (souvent moyennant finances) et ces écritures sont signées, et sont gardées éternellement dans la chaîne, qui est donc un livre des opérations, contenant tout l'historique. L'intégrité de la chaîne est garantie par la cryptographie. Toute modification est détectable par tous. Notez bien que j'ai dit **toute** modification. La chaîne ne distingue pas entre modification « légitime » ou « illégitime ». Une fois qu'une transaction est dans la chaîne, elle y est pour toujours, même si on croit avoir de bonnes raisons de l'annuler. (Oui, les techniciens vont noter que c'est plus compliqué que cela ; mais c'est **toujours** plus compliqué que cela, j'essaie d'en rester aux grandes lignes.)

Il n'y a donc pas besoin de faire confiance au Président de la Chaîne de Blocs (il n'existe d'ailleurs pas). La chaîne permet donc à des acteurs ne se connaissant pas, et ne se faisant a priori pas confiance, de travailler sur une base de données commune, consensuelle. C'est tout mais c'est énorme. La chaîne est « vérifiable par tous et contrôlée par personne ».

Les applications de la chaîne de blocs sont donc a priori nombreuses : toutes les fois où des acteurs différents faisaient appel à une autorité centrale, on pourrait mettre à la place une chaîne de blocs. L'exemple évident est la monnaie. Depuis le Moyen Âge, elle est typiquement garantie par un État

(autorité centrale). Avec la chaîne de blocs, on peut concevoir une monnaie sans autorité centrale, et c'est bien le cas de Bitcoin, la technologie qui a lancé et popularisé cette idée de **chaîne de blocs**. Outre le plaisir de se débarrasser d'une autorité centrale qui ne mérite pas forcément la confiance qu'on lui porte, cela présente des avantages comme de faciliter les micropaiements.

Donc, est-ce que tout ce qui a besoin de vérification **publique**, sans autorité centrale, est « chaînedeblocsisable » ? Prenons quelques exemples.

Après la monnaie, un autre cas de service qui est souvent géré de manière centralisé est celui de la gestion de noms (création, suppression, etc) dans un espace de nommage. Par exemple, les noms d'utilisateur de Twitter sont gérés de manière centralisée par Twitter, ce qui permet d'assurer l'unicité de ces noms (il n'y a qu'une AdrienneCharmet <https://twitter.com/AdrienneCharmet> sur Twitter). Mais cette centralisation donne aussi un contrôle excessif à Twitter : cette entreprise a pu ainsi à de nombreuses reprises fermer des comptes sur la base d'un simple signalement, souvent mensonger. La chaîne de blocs fournit une alternative : l'enregistrement des noms « premier arrivé, premier servi » peut se faire sur une chaîne de blocs, comme le fait le système Twister. Ainsi, plus personne ne peut supprimer des comptes, la censure devient bien plus difficile.

Un exemple très proche de celui-ci est celui des registres de noms de domaine. Ceux-ci enregistrent des noms de domaine, indispensables pour l'utilisation de l'Internet. Mais ils ont aussi le pouvoir de les supprimer (comme dans l'affaire Sci-Hub). On peut donc envisager de remplacer ces registres par une chaîne de blocs, où les transactions sont la création d'un nom de domaine. Le premier exemple avait été le système Namecoin, un autre exemple a été présenté par moi à la Journée du Conseil Scientifique de l'AFNIC de 2016 <https://www.afnic.fr/fr/l-afnic-en-bref/agenda/182/show/jcsa16-journee-du-conseil-scientifique-de-l-afnic-2016.html>. Attention, j'ai dit que le remplacement des registres de noms de domaine était **possible techniquement**, pas forcément qu'il était souhaitable, ni qu'il serait adopté (des tas de très bonnes idées n'ont connu aucun succès). En effet, la chaîne de blocs a aussi ses limites (voir plus loin).

Autre exemple d'application sans doute bien adaptée à la chaîne de blocs, le cadastre. Là aussi, on veut une information publique, et modifiable, et publiquement vérifiable. Au lieu de faire confiance à des autorités centrales, on pourrait tout mettre sur une chaîne de blocs. (Un exemple est souvent cité dans les médias mais sans jamais citer de source originelle donc je ne suis pas sûr qu'il soit réel.)

Dernier exemple d'une application qui est bien adaptée à la chaîne de blocs, l'enregistrement d'œuvres à des fins de prouver l'antériorité. Imaginons un artiste qui produise une vidéo, ne peut pas ou ne veut pas la publier tout de suite, mais souhaite pouvoir prouver plus tard qu'on était bien l'auteur. Même chose pour un chercheur scientifique qui est en train de rédiger un article, il ne sait pas encore quand il pourra le publier (il faut terminer certains détails, et puis le processus de publication scientifique peut être très long) mais, en cas de fuite, il veut pouvoir faire valoir son antériorité. Il existe des solutions centralisées traditionnelles, nécessitant une confiance aveugle dans un organisme comme l'INPI avec les enveloppes Soleau ou comme Ma Preuve <https://www.mapreuve.com/>. À la place, on pourrait utiliser la chaîne. Mais mettre directement leur œuvre dans la chaîne de blocs aurait deux inconvénients : cela pourrait leur coûter cher (voir plus loin les coûts de stockage dans la chaîne) et cela révèlerait leur œuvre (puisque la chaîne est publique, et lisible par tous). Une solution possible est le condensat. C'est une opération mathématique simple qui réduit (condense) un document de taille quelconque en un nombre relativement court. La condensation n'est pas inversible (à partir du condensat, on ne peut pas retrouver le contenu original). Les fonctions mathématiques utilisées ont pour propriété qu'on ne peut pas fabriquer un document ayant un condensat donné (sauf chance extraordinaire). Ainsi, si le condensat est stocké dans la chaîne de blocs, seul l'auteur original pourra, le jour venu, produire un document qui correspondra, prouvant ainsi qu'il était bien celui qui avait enregistré le condensat. J'ai développé cette idée dans mon exposé à Pas Sage en Seine 2016 <http://data.passageenseine.org/2016/mp4/

PSESHSF-2016%20-%20St%C3%A9phane%20Bortzmeyer%20-%20D%C3%A9velopper%20un%20contrat%20programme%20sur%20Ethereum.mp4> mais ce n'est pas une idée originale. Elle est également mise en œuvre dans le système Blockai <https://blockai.com>. Il a même été proposé d'utiliser une technique analogue pour faciliter le travail des historiens <https://blockchainfrance.net/2016/03/15/un-bouleversement-pour-faire-lhistoire/>.

Dans le monde de la haute technologie, un bon moyen de trier entre les techniques sérieuses et celles qui relèvent du pipeau, c'est de regarder non pas ce qu'une technique sait faire mais ce qu'elle **ne sait pas** faire. Si la description d'une technique ne liste pas ses limites, n'indique pas ce qu'elle ne peut pas faire, c'est probablement que cette technique est du pipeau. Voyons donc les cas où la chaîne de blocs n'est **pas** adaptée. D'abord, un mot sur les coûts. Comme tous les nœuds (toutes les machines du réseau) doivent exécuter les transactions (pour pouvoir les vérifier), il n'est pas exagéré de dire que « la chaîne de blocs est le plus lent et le plus cher calculateur du monde ». Pour éviter les abus, toutes les transactions doivent être payées, et le coût dépend, par exemple, de la taille des données stockées. Pas question, donc, de stocker des vidéos dans la chaîne. (Tout au plus peut-on stocker de courtes données, comme les condensats cités plus haut.) Pour la même raison, les applications qui nécessitent de longs calculs ne sont pas adaptées à la chaîne de blocs.

Celle-ci a d'autres limites : comme la chaîne est publique, il ne faut surtout pas stocker de données confidentielles. On peut parfois stocker uniquement un condensat, comme dans l'exemple plus haut, mais il faut rappeler que les métadonnées (qui stocke des données et quand, par exemple) restent visibles et qu'elles peuvent déjà beaucoup révéler. Contrairement à une légende souvent reprise par des médias sensationnalistes, la chaîne n'est pas adaptée aux transactions vraiment confidentielles. Vouloir, comme je l'ai lu dans certains articles, stocker données de santé ou fichiers scolaires est donc absurde.

La chaîne de blocs est une construction virtuelle, ne vivant que sur un réseau d'ordinateurs. Elle ne permet donc pas de contrôler des objets physiques. Ainsi, on a vu parfois des articles promettant de remplacer Airbnb par la chaîne de blocs. On peut à la rigueur gérer une serrure connectée via une application qui lit la chaîne. Mais ce n'est pas l'application qui va regarder l'état de l'appartement après le passage du locataire et faire un rapport qui influencera la réputation du locataire (une information essentielle sur Airbnb, que connaissent tous les gens qui l'ont réellement utilisé).

Cette présentation était forcément assez générale. Le monde des chaînes de blocs est en pleine effervescence et les projets sont innombrables. Parmi les propositions nouvelles, on entend souvent parler de « chaînes de blocs privées ». Souvent, ce n'est pas décrit de manière assez précise pour qu'on puisse se faire une opinion sur ces « chaînes privées ». Disons qu'une chaîne vraiment privée n'a aucun intérêt : ce serait une base de données plus lente et plus chère que les bases existantes. À la rigueur, il peut y avoir un intérêt pour des chaînes « semi-privées », par exemple au sein d'un consortium dont les membres ne se font pas confiance.

Et pour finir, un petit rappel sur des inconvénients des chaînes. Je ne veux pas dire que cette technologie est sans intérêt, bien au contraire (je ne prendrais pas la peine d'écrire sur quelque chose absolument sans intérêt). Mais elle a des limites. On a dit que toutes les transactions étaient signées, ce qui est crucial pour la sécurité de la chaîne. Mais cette sécurité repose sur la bonne gestion des clefs cryptographiques utilisées. Il faut à la fois empêcher des tiers de lire les clefs privées (pas facile sur une machine Windows infestée de logiciels malveillants) et s'assurer que ces clefs privées sont bien sauvegardées, pour faire face, par exemple, à une panne du disque dur. Cela complique sérieusement l'utilisation de la chaîne de blocs pour M. Michu ! Il existe bien sûr des solutions techniques (signatures multiples) et organisationnelles (des « notaires » à qui on sous-traiterait ce travail) à ce problème mais elles sont encore rares.

D'autre part, le caractère immuable des transactions dans la chaîne a des avantages (la censure est difficile) et des inconvénients (pas de droit à l'oubli, les transactions sont visibles éternellement...)

Merci à Michel Guillou pour ses articles <http://www.culture-numerique.fr/> et pour l'idée de celui-ci.
