Il y a des cas où la chaine de blocs n'est pas utile

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 21 octobre 2022

https://www.bortzmeyer.org/blockchain-inutile.html

La chaine de blocs, malgré quelques soubresauts et critiques, reste aujourd'hui un puissant argument marketing. On voit par exemple une université se vanter d'attester ses diplômes sur cette chaine <https://www.univ-lille.fr/fileadmin/user_upload/presse/2022/white_paper.pdf>, et son service de la communication pense apparemment que cela va jouer en sa faveur. Il est vrai que la chaine de blocs résout élégamment des problèmes auparavant considérés comme difficiles, voire impossibles, par exemple le triangle de Zooko. Mais, comme tous les outils, la chaine de blocs ne résout pas tous les problèmes. Voyons un cas où elle n'apporte rien, qui est justement le cas d'usage de l'université citée plus haut.

La chaine de blocs n'est pas simplement une liste chainée de données. Si c'était le cas, elle n'aurait rien d'intéressant, cette structure de données étant une des plus anciennes qui soit. De même, le fait que les transactions contenues dans le bloc soient signées est assez banal, les signatures numériques sont un concept ancien et répandu bien avant l'invention de la chaine de blocs. L'intérêt de la chaine de blocs est ailleurs : dans le fait qu'elle est pair-à-pair, que n'importe qui puisse y écrire, et qu'un consensus émerge entre des entités qui ne se font pas mutuellement confiance. C'est ainsi que fonctionne son utilisation la plus emblématique, les cryptomonnaies. Les gens qui acquièrent et dépensent les jetons de la cryptomonnaie utilisée ne se font pas confiance et ne se connaissent même pas. Il faut pourtant arriver à un consensus sur le fait qu'Alice ait trois jetons et, qu'après en avoir donné un à Bob, elle n'en a plus que deux (alors qu'Alice préfererait qu'on croit qu'elle en a toujours trois). C'est cela que permet la chaine de blocs et, dans ce cas d'usage, elle est irremplaçable. (Le tout est bien expliqué dans l'article <https://www.bitcoin.org/bitcoin.pdf> de Satoshi Nakamoto qui décrit le Bitcoin, et qui a intoduit le concept de chaine de blocs. Ironiquement, le terme de "*blockchain*" n'apparait pas dans cet article.)

Le but affiché des cryptomonnaies est justement de réaliser une monnaie qui ne dépende pas d'une autorité extérieure, par exemple une banque centrale. Mais si on a une telle autorité et qu'on lui fait confiance, la chaine de blocs devient inutile. Elle fonctionne toujours mais n'est pas l'utilisation la plus intelligente des ressources informatiques.

Or, c'est justement le cas de l'université citée plus haut. Pour valider des diplômes, on ne veut pas du pair-à-pair, bien au contraire. Il y a une autorité, l'université, et c'est elle, et elle seule, qui peut dire

si j'ai une maitrise de physique ou pas (mon diplôme universitaire le plus élevé). Si on met les diplômes sur une chaine de blocs, on ne souhaite certainement pas que tout le monde puisse y écrire. Le cas est donc très différent de celui des cryptomonnaies, ou d'autres utilisations de la chaine de blocs comme la réservation de noms. Notons en outre qu'aucun détail n'est donné sur la chaine utilisée par l'université : laquelle est-ce, qui la contrôle, son logiciel est-il publié, etc. En l'absence de tous ces éléments, la chaine de blocs n'apporte aucune confiance supplémentaire. L'université aurait tout aussi bien publier les diplômes sur son site Web...(Avec quelques techniques de sécurité comme HTTPS.) Et si on veut un système commun à toutes les universités, il existe déjà <https://diplome.gouv.fr/>.

Les défenseurs de ces utilisations inutiles de la chaine de blocs citent parfois l'argument de la signature, qui permet d'authentifier le diplôme, y compris si l'information circule et n'est pas récupérée sur le site d'origine. C'est vrai, les signatures numériques sont une très bonne idée, mais elles sont bien antérieures aux chaines de blocs et peuvent être utilisées dans ce cas (par exemple en publiant des documents signés sur le site Web). Là encore, la chaine de blocs n'apporte rien. Notez que le responsable du projet est parfaitement conscient de cette inutilité puisque, dans les commentaires à un article de NextInpact <https://www.nextinpact.com/article/70128/luniversite-lille-atteste-ses-diplomes-d
il dit ouvertement « j'assume que le mot blockchain a un peu été un prétexte ».

Une faiblesse courante avec les chaines de blocs est que peu de gens vérifient directement sur la chaine, pourtant la seule source fiable. Ils passent en général par un système centralisé. L'entreprise privée qui a été payée par l'université le dit d'ailleurs dans les commentaires à l'article de Next Inpact déjà cité <https://www.nextinpact.com/article/70128/luniversite-lille-atteste-ses-diplomes
« Techniquement, tout est fait dans BCdiploma pour que la lecture des attestations soit la plus simple possible en masquant la complexité de la blockchain. Par exemple, les certificats sont ici lus depuis le site de l[Caractère Unicode non montré [1]]université, augmentant ainsi la confiance. » (un exemple de ce que ça donnerait <https://diplome-certificat.univ-lille.fr/index.html?key=36CC537D863048CE
Ça annule une bonne partie de l'intérêt du projet.

Pour les mêmes raisons, tous les projets de « chaines de blocs privées » ou de « chaines à permission » sont des non-sens, en raison de leur inutilité. (À l'exception peut-être de chaines pas publiques mais pas complètement privées, entre un petit nombre d'acteurs qui ne se font qu'une confiance limitée.) Évidemment, cette inutilité n'empêche pas les projets (par exemple au niveau européen <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/FAQs>), car il y a beaucoup de consultants et d'ESN à nourrir.

Mais attention, dit la lectrice attentive de cet article : l'université peut publier des diplômes signés sur son site Web, d'accord, mais elle peut aussi arrêter de les publier. Si on fait confiance à l'université pour certifier les diplômes, mais qu'on craint qu'elle n'essaie de réécrire le passé en prétendant qu'un diplôme n'a jamais existé, la publication sur le site Web n'aide pas. Bonne remarque, et il faut donc aller plus loin que la simple publication de documents signés sur un site Web. Mais on n'a pas besoin de chaine de blocs, il suffit d'utiliser des journaux publics à ajout seul ("*append-only logs*").

Le principe de ces journaux est de publier l'information sous une forme qui rend toute altération ultérieure détectable. Il existe plusieurs solutions pour cela, mais la plus simple conceptuellement (mais pas la plus rapide) est de numéroter chaque document publié. La suppression d'un document peut ainsi être détectée. Si on a le document 67 et qu'on ne trouve pas le 66, le problème est visible. (Ce système de numérotation des documents pour assurer l'intégrité est un très vieux système, antérieur à l'informatique, avec les journaux papier utilisés par exemple dans les commissariats <https://boutique.berger-levrault.fr/documents-et-accessoires/collectivites-locales/police-municipale/

1. Car trop difficile à faire afficher par LaTeX

fonctionnement-d-un-service-de-police-municipale/registres-de-main-courante.html>. Comme le dit Wikipédia, « Il est strictement interdit de modifier ou même de raturer une inscription en main courante sous peine de la rendre caduque, c'est pourquoi les pages d'une main courante papier sont toujours numérotées. ») En dehors du monde papier, un tel système est simple à faire : l'autorité numérote les documents, les signe et les publie. Les données étant publiques, n'importe qui peut facilement vérifier leur intégrité. Un tel système est par exempe décrit dans l'article « "*How to time-stamp a digital document*" <https://dl.acm.org/doi/10.1007/BF00196791> » (à télécharger ici <https://link.springer.com/article/10.1007/BF00196791>). Un des systèmes les plus anciens à être effectivement déployé est Stamper <http://www.itconsult.co.uk/stamper.htm> (cf. son historique <https://www.itconsult.co.uk/stamper/stampnew.htm>), qui publiait ses signatures (faites avec PGP)...sur Usenet.

Depuis, bien d'autres systèmes de journaux à ajout seul sont apparus et sont utilisés. L'un des plus connus est le "*Certificate Transparency*" (normalisé dans le RFC 9162[2]). Pas du tout besoin d'une chaine de blocs pour cette tâche cruciale, puisqu'il n'y a qu'un petit nombre d'émetteurs faisant autorité (les AC).

Au passage, j'ai dit qu'un tel système permettait de détecter les modifications. Or il y a des modifications légitimes, par exemple le retrait d'un diplôme obtenu à tort. Il faut donc prévoir la possibiité qu'un document annule un précédent (mais on ne supprime pas le précédent, on le remplace). La vérification publique est contradictoire avec la possibilité d'oubli, ce qui peut être une bonne ou une mauvaise chose.

2. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc9162.txt