

Depuis quelques années, il est devenu possible de disposer de l'équivalent d'une horloge de référence sans avoir à craindre qu'elle puisse être utilisée en avance. La méthode publiée en 2018 par Jia Liu, Tibor Jager, Saqib Kakvi et Bogdan Warinschi s'appuie sur les blockchains (ou chaînes de blocs) publiques, comme celle de la monnaie cryptographique Bitcoin en fonctionnement depuis 2009.

La blockchain du Bitcoin est un fichier recopié à l'identique en chaque nœud d'un réseau informatique, ce fichier étant géré et surveillé par chaque nœud de ce réseau. Le fichier évolue toutes les dix minutes environ par l'ajout d'une nouvelle page (ou bloc) et c'est cet ajout périodique qui fixe l'avancée de l'horloge. Son fonctionnement n'est pas extrêmement précis, car l'intervalle de dix minutes n'est qu'une moyenne.

UNE BLOCKCHAIN POUR UNE HORLOGE DÉCENTRALISÉE

Cependant, cette horloge décentralisée n'est aux mains de personne en particulier. C'est donc l'ensemble des nœuds du réseau, environ 10 000 répartis dans le monde entier, qu'il faudrait soudoyer pour fausser le signal qu'elle émet. En perturber le fonctionnement est pratiquement impossible, car l'ajout d'une nouvelle page exige que le réseau fasse une quantité colossale de calculs, aujourd'hui environ 10^{20} calculs de la fonction SHA256 par seconde. Il y a donc bien, comme pour les méthodes proposées par Adi Shamir et ses collègues, un calcul important à faire qui régule l'horloge. Cependant, la situation est très différente pour trois raisons rassurantes.

Tout d'abord, ce ne sont pas ceux qui créent ou veulent lire le contenu des capsules temporelles en s'appuyant sur cette horloge qui font les calculs, mais les nœuds du réseau qui sont motivés par les gains payés en nouveaux bitcoins créés pour cette participation au fonctionnement du réseau.

Ensuite, la difficulté du calcul à mener pour faire avancer l'horloge d'une étape de dix minutes se réajuste automatiquement tous les

quatorze jours pour prendre en compte l'évolution de la capacité totale du réseau : la difficulté augmente si le réseau a accru sa capacité à calculer, elle diminue sinon. Ce réajustement annule l'évolution de puissance du réseau et maintient sur le long terme la durée moyenne d'une étape à dix minutes. Les progrès de l'électronique, ou d'autres natures n'accéléreront pas l'horloge.

Enfin, quelqu'un qui voudrait seul accélérer brusquement le calcul pour produire de nombreuses étapes rapprochées de l'horloge doit disposer d'une capacité de calcul propre de l'ordre de grandeur de celle cumulée de tous les nœuds validateurs du réseau, ce qui est très difficile à imaginer. Une dernière raison rend improbable la manipulation de l'horloge du bitcoin par un seul acteur : celui qui pourrait le faire pourrait aussi exploiter cette capacité de calcul pour s'approprier une grande partie des nouveaux bitcoins créés, dont la valeur équivaut à plusieurs milliards de dollars par an... ce qu'il préférera sans doute !

La blockchain semble donc nous approcher de l'idéal souhaité. Le système ne repose pas sur des tiers de confiance et il assure l'anonymat des créateurs de capsules temporelles et de ceux qui veulent les lire. Le message secret circule et se libère indépendamment de celui qui l'a émis, personne qui peut avoir disparu au moment de l'ouverture. Et lire le message une fois la date atteinte ne demande pas de capacité de calcul particulière et n'exige pas de s'en être occupé depuis son émission.

D'autres idées s'appuyant sur la notion de *smart-contract* du réseau Ethereum ont aussi été proposées. Ces méthodes ne sont malheureusement sans doute pas assez sûres à très long terme. En effet, comment être certain que, dans dix ans ou plus, les réseaux Bitcoin et Ethereum continueront de fonctionner, qu'ils auront résisté à toutes les attaques et n'auront pas été délaissés pour de meilleurs modèles de blockchain ?

Le problème est difficile, mais la science cryptographique avance, en produisant d'année en année d'étonnants résultats ! ■

BIBLIOGRAPHIE

W.-J. Lai et al., **A fully decentralized time-lock encryption system on blockchain**, 2019 *IEEE International Conference on Blockchain*, IEEE, 2019.

G. Branwen, **Time-Lock Encryption**, 2019 (<https://www.gwern.net/Self-decrypting-files>).

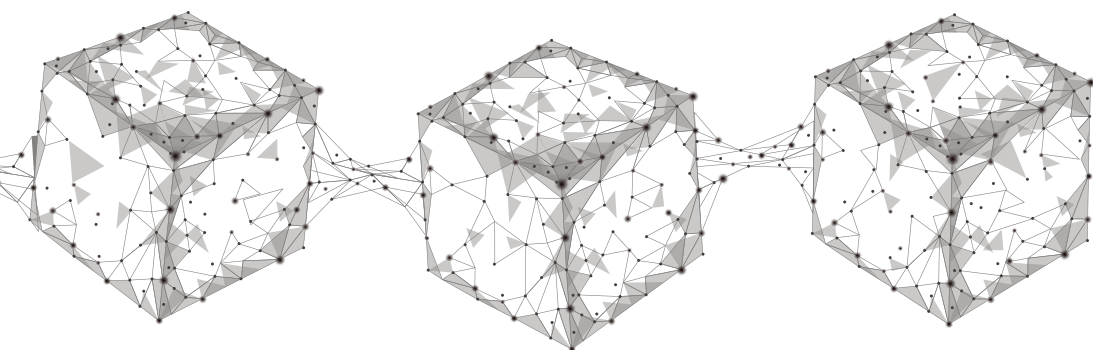
J. Liu et al., **How to build time-lock encryption**, *Designs, Codes and Cryptography*, vol. 86, pp. 2549-2586, 2018 (<https://bit.ly/36Rrx0u>).

J. Cathalo et al., **Efficient and non-interactive timed-release encryption**, *International Conference on Information and Communications Security*, Springer, 2005.

A. Chan et I. F. Blake, **Scalable, server-passive, user-anonymous timed release cryptography**, 25th *IEEE International Conference on Distributed Computing Systems (ICDCS'05)*, IEEE, 2005.

R. Rivest, **Description of the LCS35 Time Capsule Crypto-Puzzle**, 1999 (<https://bit.ly/3jKRQt1>).

R. Rivest et al., **Time-lock puzzles and timed-release crypto**, Technical Report MIT/LCS/TR-684, MIT Laboratory for Computer Science, 1996 (<https://bit.ly/3nvd72>).



LES AUTEURS

JEAN-MICHEL COURTY et ÉDOUARD KIERLIK
professeurs de physique à Sorbonne Université, à Paris

BENOÎT SEMIN
chercheur CNRS au laboratoire PMMH (Physique
et mécanique des milieux hétérogènes), à Paris

BIEN VENTILER POUR BIEN RESPIRER

Pour limiter la propagation du Covid-19, il faut aérer les lieux clos. Mais quand et pendant combien de temps ? Pour répondre, à défaut de mesurer la quantité de microbes dans l'air, on peut s'appuyer sur la concentration de dioxyde de carbone de l'air que l'on respire.



Renouveler l'air dans les lieux clos: ce thème a resurgi dans le débat public avec la pandémie de Covid-19. En effet, le virus impliqué se transmet notamment par voie aérienne, d'où la recommandation actuelle de bien ventiler les lieux clos pour contrer sa propagation. Cependant, bien au-delà de la crise épidémique, une bonne ventilation est importante pour la santé et le bien-être en général. Comment s'assurer qu'elle est satisfaisante ? En mesurant le taux de dioxyde de carbone, le CO_2 , dans l'air. Ce gaz carbonique est produit par notre respiration et son taux permet donc d'estimer la qualité de l'aération.

ÉVITER DE DÉPASSER 1000 PPM DE CO_2

Dans l'air extérieur, la concentration moyenne de CO_2 est d'environ 0,04%, c'est-à-dire que 1 molécule sur 2500 est une molécule de CO_2 . Pour éviter d'avoir à manipuler des chiffres décimaux, on utilise plutôt la «partie par million», ou ppm en abrégé: on a donc ici une concentration d'environ 400 ppm, avec, en ville, des variations de quelques dizaines de ppm

dues à la pollution ou à la situation météorologique.

Lorsque nous sommes à l'extérieur, l'air que nous expirons se dilue rapidement dans l'immensité de l'air ambiant; notre respiration n'a donc aucune conséquence sur la concentration de CO_2 . Tel n'est pas le cas dans un espace clos. Dans l'air expiré, la concentration de CO_2 atteint environ 40 000 ppm (soit 4%). On estime ainsi que lors d'une respiration normale, un adulte rejette 18 litres de CO_2 par heure à pression atmosphérique. Dans un espace clos, la concentration de CO_2 augmente donc progressivement.

Pour fixer les idées, considérons une pièce où chaque personne dispose de 10 mètres cubes d'air. Cela correspond par exemple à 5 personnes dans un salon de 20 mètres carrés et 2,5 mètres de hauteur. Si la pièce est étanche et non ventilée, la concentration de CO_2 augmente linéairement avec le temps. Au bout de 1 heure, 18 litres de CO_2 s'ajouteront aux 10 mètres cubes (soit 10 000 litres) d'air par personne: la concentration sera donc augmentée de 1800 ppm et atteindra 2200 ppm si l'air de la pièce avait initialement la même composition que l'air extérieur.

Dans un lieu clos, la respiration des personnes présentes accroît assez vite la concentration en CO_2 de l'air. Pour rester à moins de 1500 ppm de CO_2 dans une salle offrant une dizaine de mètres cubes d'air par personne, il faut renouveler l'air à peu près toutes les demi-heures. À cette fin, ouvrir grand les fenêtres quelques minutes suffit.

Or des études ont montré qu'au-delà d'une teneur en CO_2 de 2000 ppm, nos capacités cognitives commencent à s'altérer, et cela d'autant plus qu'elles sont de niveau élevé (prise de décision, réflexion...). C'est pourquoi les valeurs maximales conseillées pour la concentration de CO_2 en intérieur se situent d'habitude entre 1000 et 1500 ppm; elles s'appliquent notamment aux bâtiments résidentiels et aux bureaux.

Comment ne pas dépasser ces seuils ? Par exemple en faisant appel à une ventilation mécanique. La norme européenne de ventilation dans les locaux non résidentiels (EN 13779) préconise un débit de 29 mètres cubes par heure et par personne pour que la qualité de l'air soit «modérée». D'où sort ce chiffre ?

Après une phase transitoire où elle varie, la teneur en CO_2 se stabilise lorsque