

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>).

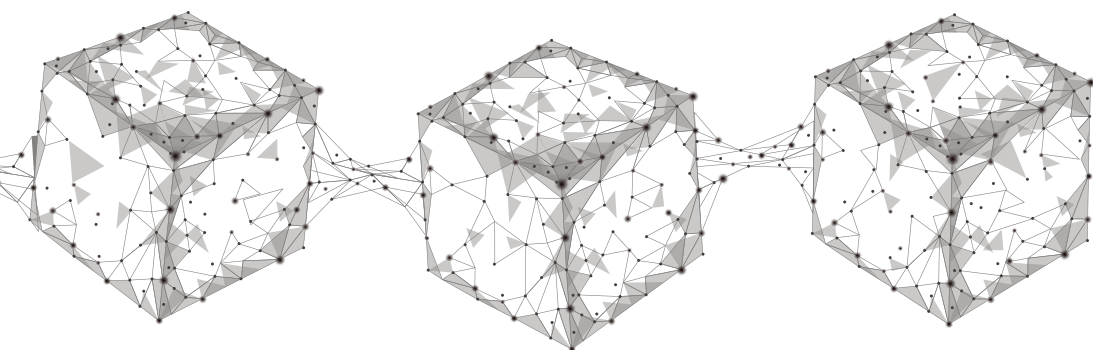
J. Liu et al., **How to build time-lock encryption**, *Designs, Codes and Cryptography*, vol. 86, pp. 2549-2586, 2018 (<https://bit.ly/36Rrx0u>).

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/3nvdu72>).



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.

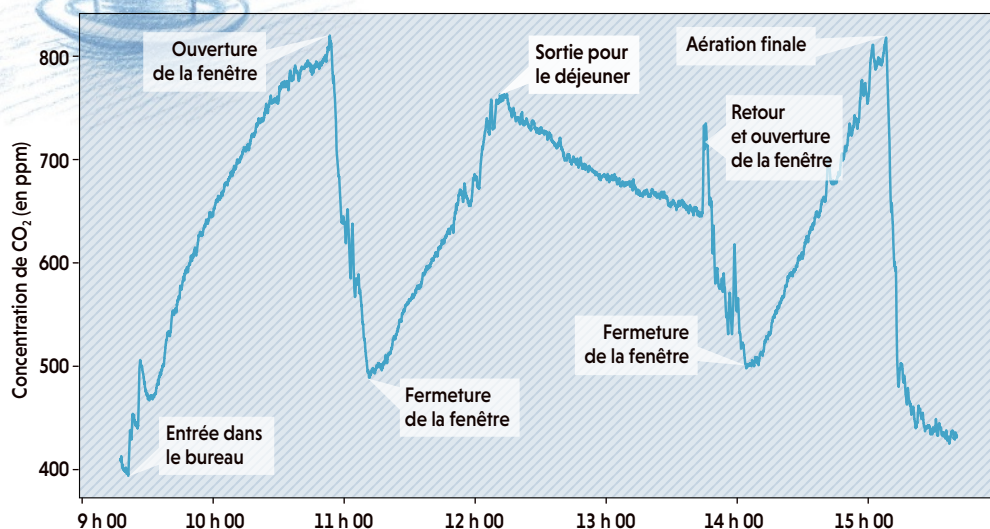
Comment ne pas dépasser ces seuils ? Par exemple en faisant appel à une ventilation mécanique. La norme européenne de ventilation dans les locaux non résidentiels (EN 13779) préconise un débit de 29 mètres cubes par heure et par personne pour que la qualité de l'air soit « modérée ». D'où sort ce chiffre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

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



ÉVOLUTION RAPIDE DE LA TENEUR EN CO₂

Dans un lieu clos, la concentration en CO₂ de l'air augmente vite lorsque des personnes sont présentes, chaque adulte rejetant, par sa respiration, environ 18 litres par heure de ce gaz à pression atmosphérique. Mais l'ouverture des fenêtres permet de revenir très rapidement à une concentration normale. C'est ce qu'illustre le graphique ci-dessous, issu des mesures par l'un des auteurs (Jean-Michel Courty) de la teneur en CO₂ dans son bureau, au fil de ses allées et venues et des ouvertures et fermetures de la fenêtre.



le gaz carbonique produit par la respiration est évacué à chaque instant par la ventilation. Or cette quantité évacuée, en supposant que l'air est suffisamment brassé pour être homogène, n'est autre que le produit du débit de la ventilation par la concentration en CO₂. On trouve donc que, en régime stationnaire, la concentration de CO₂ est égale à la somme de la concentration atmosphérique (400 ppm) et du rapport du débit produit sur le débit évacué. Ainsi, 18 litres de CO₂ par heure sur 29 mètres cubes d'air par heure donnent un supplément de 620 ppm de CO₂, d'où une concentration totale de 1020 ppm.

Ce chiffre est acceptable, mais il frôle déjà les maxima recommandés. Remarquons aussi que ce résultat, et donc le dimensionnement d'une ventilation, ne dépend pas du volume de la pièce, mais seulement du nombre de ses occupants. Le respect de la norme nécessite donc d'estimer l'occupation maximale des locaux.

AÉRER QUELQUES MINUTES TOUTES LES DEMI-HEURES

En l'absence de ventilation mécanique, il reste l'aération naturelle. Pour en revenir à l'exemple d'une personne dans 10 mètres cubes d'air, on atteint

1300 ppm de CO₂ au bout d'une demi-heure; il faut alors ouvrir grand les fenêtres pour renouveler complètement l'air de la pièce. Plusieurs mécanismes peuvent y contribuer: le vent, bien entendu, mais aussi la différence de température entre l'intérieur et l'extérieur. Celle-ci engendre des différences de densité de l'air et des mouvements de >

Les auteurs ont notamment publié: **En avant la physique!**, une sélection de leurs chroniques (Belin, 2017).



> convection ascendants et descendants à travers les ouvertures.

Il est cependant beaucoup plus difficile d'estimer les débits correspondants. En égalant la force ascensionnelle qui s'exerce sur l'air chaud et le frottement aérodynamique avec l'air ambiant, on calcule des vitesses de l'ordre de 0,5 mètre par seconde pour des écarts de température de 10 °C. En supposant que la moitié de la surface des fenêtres, disons 4 mètres carrés pour notre salon de 20 mètres carrés, permet de faire rentrer de l'air de l'extérieur tandis que l'autre moitié sert à évacuer l'air vicié, on renouvelerait totalement les 50 mètres cubes d'air du salon en 50 secondes grâce à un débit phénoménal de 3600 mètres cubes par heure.

Cette estimation de débit est un peu trop élevée, et ce temps trop court, mais ces chiffres suggèrent ce que chacun a pu vérifier, à savoir que la convection naturelle parvient à renouveler l'air d'une pièce en quelques minutes. Cette durée est d'ailleurs suffisamment brève pour éviter, l'hiver, de refroidir les meubles et les murs; le confort thermique n'est par conséquent que momentanément perturbé! Mais tout cela suppose que la convection soit possible: sans vent et sans grand écart de température, il faut se résigner, à la mi-saison, à laisser les fenêtres ouvertes en permanence pour aérer.

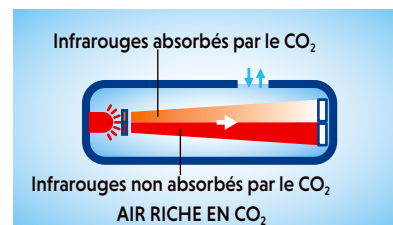
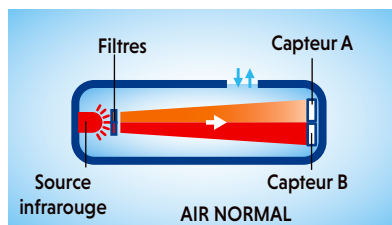
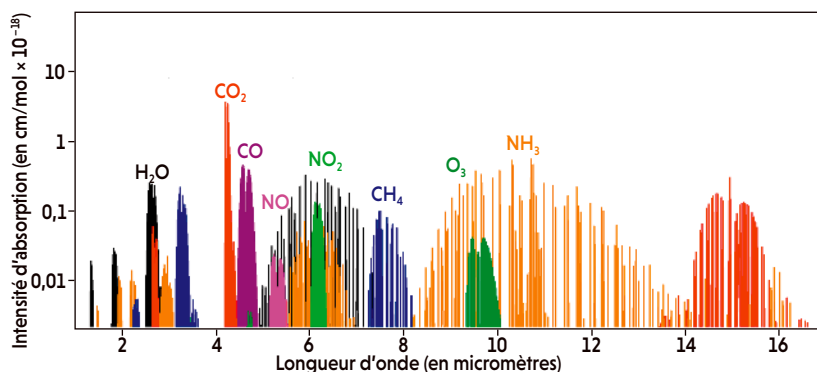
MESURER LA TENUEUR EN CO₂

Comment s'assurer que le renouvellement de l'air est suffisant? Dans l'industrie du bâtiment, un contrôle standard consiste à mesurer le taux de CO₂ de l'air intérieur. S'il existe des appareils à usage professionnel, on trouve désormais dans le commerce des détecteurs peu coûteux que l'on peut piloter avec une carte Arduino. Ces appareils, qualifiés de NDIR (pour *non dispersive infrared spectroscopy*, «spectroscopie infrarouge non dispersive»), mesurent l'absorption de la lumière infrarouge par les molécules de l'air.

En effet, le gaz carbonique absorbe les infrarouges autour d'une longueur d'onde de 4,3 micromètres, qui excite des modes de vibration de ses liaisons carbone-oxygène. Cette valeur est éloignée des bandes spectrales d'absorption des autres molécules de l'air, telles que le dioxygène (O₂), le monoxyde de carbone (CO) et l'eau: la mesure de l'absorption est donc très sélective (voir l'encadré ci-dessus). À 400 ppm de CO₂, l'intensité

DÉTECTER LE CO₂ AVEC DES INFRAROUGES

Le dioxyde de carbone présente un pic d'absorption du rayonnement à 4,3 micromètres de longueur d'onde, dans l'infrarouge. Ce pic d'absorption est bien séparé de ceux des autres gaz présents dans l'atmosphère (voir le graphique) et offre donc un moyen commode de détecter le CO₂ et de mesurer sa concentration. Les détecteurs NDIR comportent ainsi deux capteurs, l'un, A, opérant à la longueur d'onde du pic d'absorption, l'autre, B, opérant à d'autres longueurs d'onde, non absorbées (voir le schéma). Ainsi, le signal du capteur A dépend de la concentration en CO₂ de l'air traversé par le faisceau infrarouge, tandis que le capteur B produit un signal indépendant de cette concentration. Grâce à cette détection différentielle, les appareils NDIR mesurent la concentration de CO₂. Contrairement à d'autres types de détecteurs de CO₂, ils ne nécessitent pas de recalibrage régulier et restent opérationnels pendant plusieurs années.



d'un rayonnement vers 4 micromètres de longueur d'onde diminue de 2 % au bout de 5 centimètres. Cela semble peu, mais il faut s'en contenter si l'on veut un dispositif de mesure de petite taille.

C'est pourquoi les bons détecteurs NDIR effectuent des mesures différentielles. Ils comportent une source émettant dans l'infrarouge et deux capteurs, l'un sensible aux longueurs d'onde non absorbées par le CO₂ et qui sert de référence, l'autre sensible autour de la longueur d'onde de 4,3 micromètres, absorbée par le CO₂. L'intensité reçue par le second capteur varie donc avec la concentration de CO₂, contrairement à celle reçue par le premier, et la différence permet de déterminer la concentration de CO₂. Ainsi, avec un tel appareil que l'on trouve pour quelques dizaines d'euros, chacun peut vérifier si l'air qu'il respire est suffisamment renouvelé. ■

BIBLIOGRAPHIE

R. K. Bhagat et al., **Effects of ventilation on the indoor spread of COVID-19**, *Journal of Fluid Mechanics*, vol. 903, F1, 2020.

U. Satish et al., **Is CO₂ an indoor pollutant ? [...]**, *Environ. Health Perspect.*, vol. 120(12), pp. 1671-1677, 2012.

J. Hodgkinson et R. P. Tatam, **Optical gas sensing : A review**, *Meas. Sci. Technol.*, vol. 24(1), 012004, 2012.

P. F. Linden, **The fluid mechanics of natural ventilation**, *Annu. Rev. of Fluid Mech.*, vol. 31, pp. 201-238, 1999.

L'UNIVERS AVANT LE BIG BANG

- 7 dossiers rédigés par des chercheurs et des experts sur le sujet
- Une lecture adaptée sur écrans

3,99 €



Les *Thema* sont une collection de hors-séries numériques. Chaque numéro contient une sélection des meilleurs articles publiés dans *Pour la Science* sur une thématique.

Dans la collection *Thema* découvrez aussi



**Commandez et téléchargez
les numéros en pdf**



Pour lire votre numéro, rendez-vous dans votre compte client



boutique.pourlascience.fr/tous-les-numeros/thema.html