> Pour atteindre l'objectif recherché, on peut s'appuyer sur les techniques d'« offuscation » de programmes et sur l'existence d'horloges publiques sécurisées ou aux propriétés particulières.

DES PROGRAMMES OFFUSQUÉS QUI SURVEILLENT L'HEURE

L'offuscation de programmes consiste à écrire des programmes informatiques que tout le monde peut avoir et faire fonctionner, mais dont la logique de fonctionnement est tellement embrouillée et masquée que même en étudiant soigneusement le programme, on ne saura pas bien ce qu'il fait. Cela empêche qu'on les modifie ou qu'on exploite les idées qui ont conduit à leur mise au point.

Si l'on maîtrise l'offuscation, on peut créer un programme à retardement livrant un message à une date fixée par le créateur: une fois lancé sur une machine ayant accès à internet, le programme offusqué lit l'heure sur un ou plusieurs sites qui la publient en continu. Quand l'heure trouvée dépasse la date programmée, le programme déchiffre l'information qui est cachée en lui et la fait alors apparaître en clair. Si l'information qu'on veut libérer est très volumineuse, l'information libérée sera la clé de déchiffrement du fichier chiffré contenant cette information, le programme offusqué ne servant qu'à cacher la clé de déchiffrement.

Il existe de nombreux sites publiant l'heure, en particulier l'horloge parlante (http://www.horlogeparlante.com). On peut imaginer qu'ils fonctionneront encore longtemps et suivront le même mode de publication. Si l'on craint qu'ils soient compromis ou simplement arrêtés, l'utilisation de plusieurs horloges dispersées en des endroits divers du monde fournira une garantie renforcée. Le programme consultera par exemple n horloges et considérera comme certain que le moment attendu est atteint seulement si k horloges parmi n l'indiquent.

Cette méthode est moins risquée que celle où l'on confie le message à un tiers de confiance: les horloges utilisées ne sont pas informées du message caché dans le programme offusqué, et ne savent même pas qu'on les utilise. Toutefois, certains résultats théoriques semblent indiquer qu'aucune méthode parfaite d'offuscation n'existe. D'autres résultats récents utilisant une définition moins stricte de l'offuscation montrent qu'on peut réussir, mais au prix d'un ralentissement du fonctionnement du programme offusqué.

C'est pourquoi on a recherché des méthodes ne faisant pas appel à l'offuscation. L'une d'elles, décrite en 2004 par Aldar Chan et Ian Blake, et perfectionnée en 2006 par Julien Cathalo, Benoît Libert et Jean-Jacques Quisquater, décrit comment une horloge de référence fiable peut produire et publier des informations qui permettront à quelqu'un voulant émettre un message à retardement de le faire sans que l'horloge ait à connaître le message temporairement chiffré ni même savoir qu'un tel message existe.

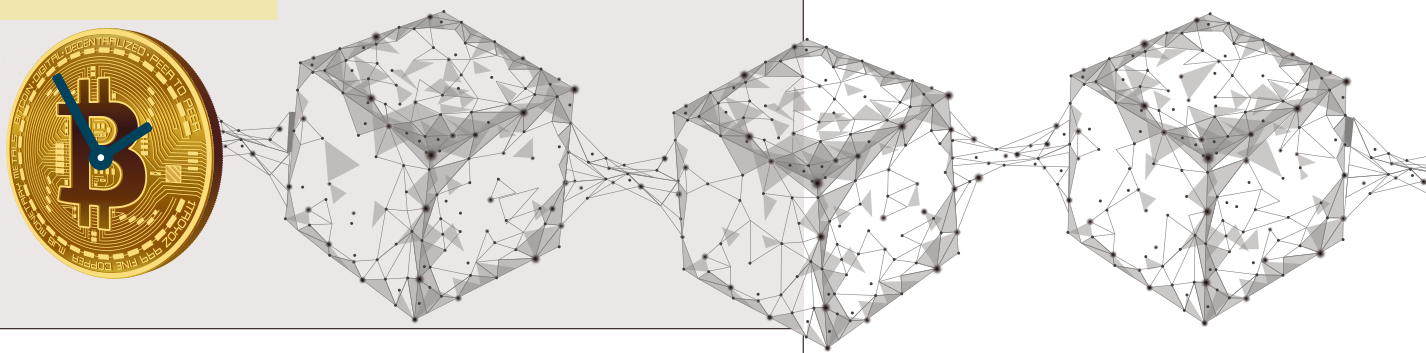
L'horloge produit à la date voulue des informations permettant de déchiffrer les fichiers secrets. Ni le créateur de la capsule temporelle ni ceux à qui elle est adressée n'ont à interagir avec l'horloge qui diffuse les messages permettant de déchiffrer les capsules temporelles ayant atteint l'instant de libération. Ces méthodes permettent aussi de préserver l'anonymat des utilisateurs qui créent les capsules temporelles ou les lisent l'heure venue.

Malheureusement, celui qui fait fonctionner horloge peut produire avant l'heure les clés de déchiffrement des capsules temporelles. La solution est donc encore imparfaite.

5 LA SOLUTION BLOCKCHAIN

La technologie des blockchains qui est utilisée pour émettre et faire circuler des cryptomonnaies telles que le Bitcoin met à la disposition de tous une horloge décentralisée dont le fonctionnement ne peut être perturbé par personne.

Cette technologie permet de concevoir des capsules temporelles dont la sûreté n'est pas liée à la confiance accordée à un acteur particulier. Cette dernière avancée dans la conception de capsules temporelles de plus en plus proches de l'idéal, décrit dans l'encadré 2, est due à Jia Liu, de l'université de Surrey, Tibor Jager et Saqib Kakvi, de l'université de Paderborn, et Bogdan Warinschi, de l'université de Bristol, et a été publiée en 2018 ***(voir la bibliographie)*****.**



© Shutterstock.com/Iurii Motov/LuckyStep

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.

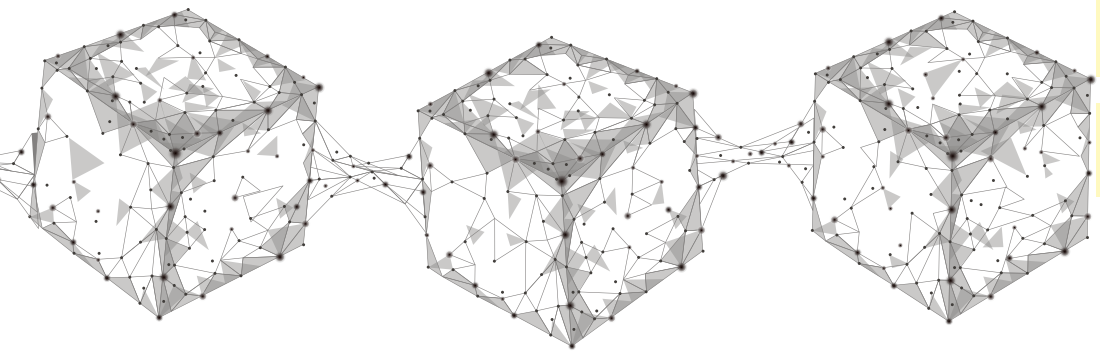
Ensuite, la difficulté du calcul à mener pour faire avancer l'horloge d'une étape de dix minutes se réajuste automatiquement tous les quatorze jours pour prendre en compte l'évolution de la capacité totale du réseau: la difficulté augmente si le réseau a accru sa capacité à calculer, elle diminue sinon. 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).