

infalsifiables et vérifiables *a posteriori*. L'utilisation de fonctions de hachage au sein des pages ajoutées périodiquement aux fichiers blockchains semble introduire un hasard dans ces blockchains qui par ailleurs sont publiques et infalsifiables car conservées en de multiples exemplaires lisibles par tous. Cependant, une étude publiée en 2018 par Cécile Pierrot, de Sorbonne Université, à Paris, et Benjamin Wesolowski, de l'École polytechnique fédérale de Lausanne (EPFL), a montré qu'en réalité de telles sources pourraient être manipulées par des acteurs assez puissants. Même si cela peut avoir un certain intérêt d'utiliser l'aléa des blockchains en le mêlant à d'autres sources, une balise aléatoire ne doit pas se fonder sur cette méthode seule.

Plus intéressant, le cryptologue Arjen Lenstra, de l'EPFL, et Benjamin Wesolowski, ont récemment introduit deux idées nouvelles susceptibles de renforcer la confiance envers les balises aléatoires modernes.

La première idée est de permettre aux acteurs qui le souhaitent de participer à ce qui est produit. Entre deux émissions successives, on permettrait à quiconque le souhaite d'envoyer des nombres à la balise. Tous ces nombres seraient regroupés en un seul dont on calculerait l'empreinte, et l'on mêlerait celle-ci aux résultats du mécanisme local (quantique ou autre) de la balise, par exemple par le biais d'une somme modulo 2 comme quand on mélange plusieurs balises. De plus, le site de la balise autoriserait la vérification que les nombres envoyés sont bien pris en compte.

Le fait de pouvoir envoyer ses propres données assurerait que, même si tous les autres intervenants et la balise forment une association dont le but est de vous tromper, elle ne réussira pas. Le fait que vous interveniez ne vous donne heureusement pas le pouvoir de manipuler la balise et cela même en vous coordonnant avec tous les intervenants extérieurs, car la composante locale (avec une somme modulo 2) rend vaine toute tentative de biais.

DES FONCTIONS DONT LE CALCUL NÉCESSITE UN DÉLAI

La seconde idée est plus subtile, mais la plus importante peut-être pour assurer qu'aucune manipulation n'est possible, même par la balise. Elle utilise le concept de *fonction vérifiable à délai* ou VDF (le sigle anglais), objet d'intenses recherches depuis trois ans.

Une VDF est une fonction qui, lorsqu'on lui confie un fichier quelconque, le transforme en une séquence de chiffres aléatoires, comme le fait une fonction de hachage (voir l'encadré 3). Mais en plus, elle le fait de telle façon que le calcul ne peut pas être mené en moins d'une certaine durée (par exemple 30 secondes), et que la vérification de son

résultat final est quasi instantanée: calculer est long, vérifier est rapide.

Même si une balise aléatoire combine des sources extérieures, selon la première idée, un problème persiste qu'une VDF va résoudre. Le problème est qu'au moment où la balise mélange les données extérieures (qu'elle ne contrôle pas) et une donnée locale, par exemple présentée comme quantique, elle pourrait s'arranger, connaissant les données extérieures, pour que la combinaison avec ce qu'elle introduit (prétendument tiré d'un mécanisme quantique), conduise à un résultat final biaisé comme elle le souhaite. En clair, à cause de la donnée locale qu'elle introduit, la balise garde une possibilité de tricherie. Comment rendre impossible cette manipulation?

Voici la solution d'Arjen Lenstra et Benjamin Wesolowski. La balise exige que les données externes qu'elle prendra en compte lui soient parvenues durant les 30 premières secondes de l'intervalle de temps de 60 secondes entre deux émissions (en t , et en $t+60$). Elle-même, à l'instant $t+30$, engage sa donnée (par exemple quantique) en publiant son empreinte. La balise combine les données extérieures et la sienne et, à partir du résultat, effectue le calcul de la VDF qui exige 30 secondes. Le résultat de ce calcul est connu et publié par la balise à l'instant $t+60$ (il ne peut pas l'être avant) avec la donnée dont la balise n'avait communiqué que l'empreinte à l'instant $t+30$. Tout le monde peut vérifier instantanément que le calcul fait par la balise est correct (c'est la propriété de vérifiabilité instantanée) et qu'elle n'a pas changé sa donnée (puisque'elle en avait publié l'empreinte).

Les acteurs extérieurs n'ont pas pu agir sur le résultat, car ils ne connaissaient pas la donnée de la balise, restée secrète jusqu'à $t+60$, et que le résultat en dépend.

Plus important, la balise n'a pas pu proposer une donnée conduisant à un résultat qui l'arrange. En effet, dès l'instant $t+30$, elle a figé la donnée qu'elle proposait (en publiant l'empreinte) et il lui a fallu 30 secondes pour savoir comment cette donnée combinée aux autres données venant de l'extérieur (qu'elle ne connaissait pas entièrement avant $t+30$) produisait le résultat. Dans le protocole, ni un fournisseur de données externes ni la balise elle-même ne peuvent tricher. Le résultat dépend de toutes les données et il est donc vraiment aléatoire, si un seul des fournisseurs de données (local ou externe) en livre qui soient aléatoires.

On dispose ainsi de méthodes cryptographiques pour concevoir et réaliser des balises aléatoires fiables et sécurisées. Rien ne semble interdire ou limiter les applications exigeant des balises parfaitement sécurisées. On peut désormais exiger des sites internet de jeux, des loteries et lotos divers qu'ils se fondent de manière transparente sur de telles balises. ■

BIBLIOGRAPHIE

K. Pietrzak, **Simple verifiable delay functions**, *IACR Cryptology ePrint Archive*, n° 627, 2018.

D. Boneh et al., **Verifiable delay functions**, dans H. Shacham et A. Boldyreva (éd.), *Advances in Cryptology – CRYPTO 2018*, Springer, 2018.

C. Pierrot et B. Wesolowski, **Malleability of the blockchain's entropy**, *Cryptography and Communications*, vol. 10(1), pp. 211-233, 2018.

A. Lenstra et B. Wesolowski, **Trustworthy public randomness with sloth, unicorn, and trx**, *Int. J. of Appl. Crypt.*, vol. 3(4), pp. 330-343, 2017.

J. Bonneau et al., **On Bitcoin as a public randomness source**, *IACR Cryptology ePrint Archive*, n° 1015, 2015.

La balise aléatoire de Mads Haarh : www.random.org

La balise aléatoire du NIST : <https://beacon.nist.gov>

La balise aléatoire de l'université du Chili : <https://random.uchile.cl/en/>

Un site collectant les derniers travaux sur les VDF : <https://vdfresearch.org/>

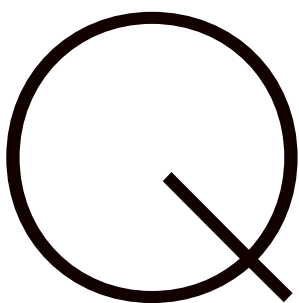
L'AUTEUR



LOÏC MANGIN
rédacteur en chef adjoint
à Pour la Science

OÙ SE CACHE LE TRIFLUOROMÉTHYLE ?

Un artiste-plasticien rend hommage à un nouveau type de réaction chimique, respectueux de l'environnement, qui aidera à préparer des composés inédits comportant un groupe trifluorométhyle, souvent intéressant en pharmacologie.



u'ont en commun l'antidépresseur Prozac, l'antipaludéen Lariam, l'anti-VIH Sustiva... ? Outre leur effet dirigé contre quelque chose, leurs principes actifs (respectivement fluoxétine, méfloquine, éfavirenz et fipronil) sont tous dotés d'un groupe chimique trifluorométhyle (CF_3). À la liste précédente, on aurait pu ajouter un autre « produit » qui partage cette particularité : une œuvre récente (voir page ci-contre) de Patrick Barrès, enseignant-chercheur au Laboratoire de recherche en audiovisuel – savoirs, praxis et poétiques en art, à l'université de Toulouse ! Où est le trifluorométhyle ?

Tout commence dans les laboratoires de Géraldine Masson, de l'Institut de chimie des substances naturelles, à l'université Paris-Saclay, et celui d'Emmanuel Magnier, de l'institut Lavoisier, à l'université de Versailles-Saint-Quentin. Avec leurs collègues, ils ont récemment mis au point une méthode de synthèse de composés trifluorométhylés, à l'aide de réactions plus respectueuses de l'environnement.

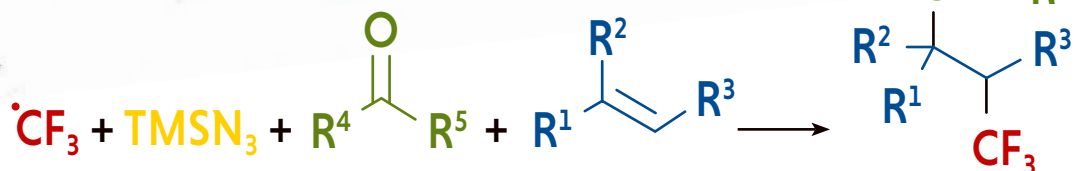
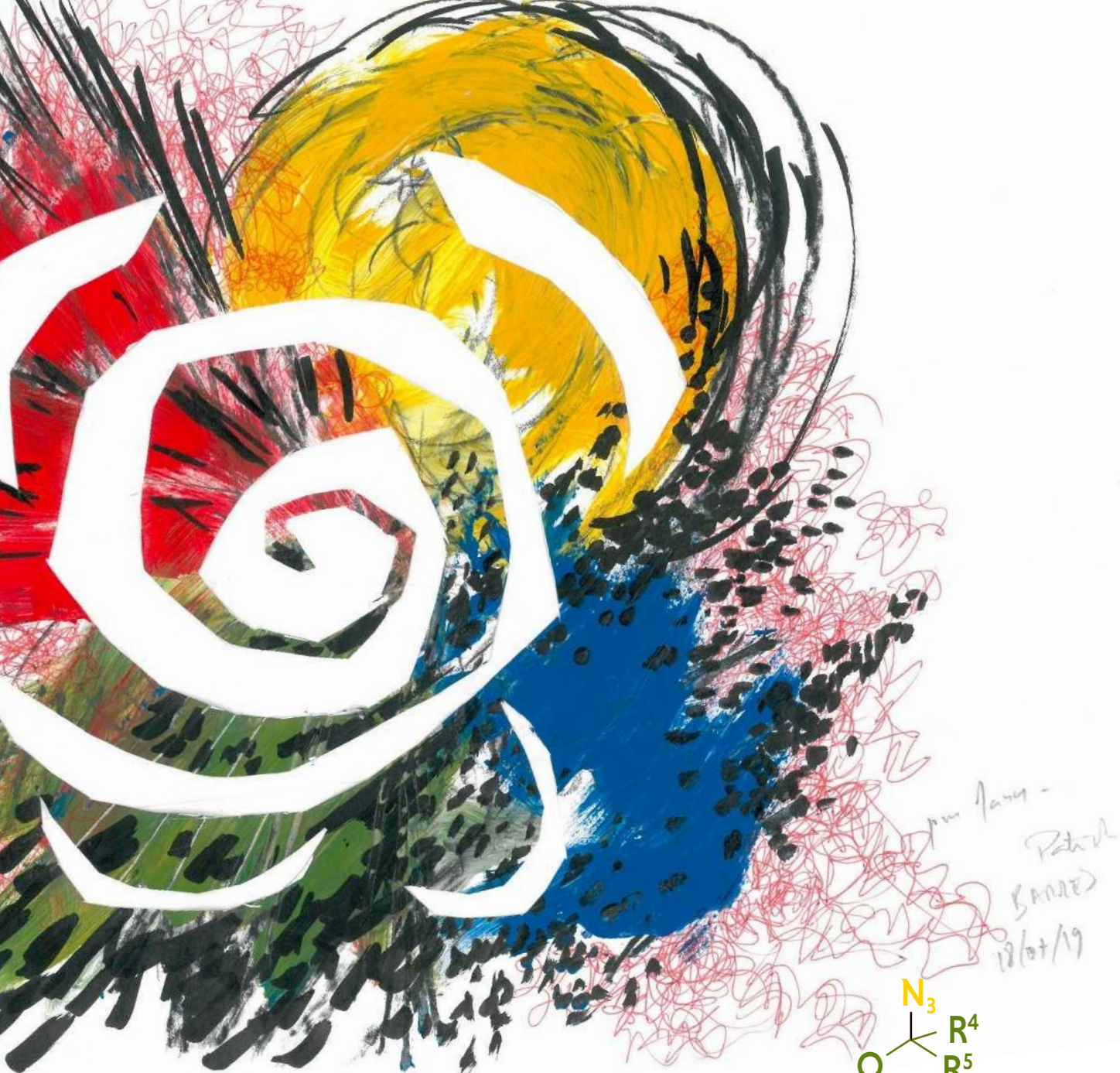
La piste suivie est celle de la photocatalyse d'oxydo-réduction dont l'un des pionniers fût, au début des années 1980, par Alain Deronzier, de l'université de Grenoble. L'idée est d'utiliser un photocatalyseur qui, éclairé, passe dans un état excité et peut alors donner ou recevoir un électron et ainsi démarrer une réaction, voire plusieurs, et dans le cas qui nous intéresse un processus dit « radicalaire » (un seul électron est engagé).

Patrick Barrès s'est emparé du résultat des chimistes et a souhaité le représenter symboliquement. De fait, les quatre zones colorées correspondent à autant de

réactifs mis en jeu : des alkènes, c'est-à-dire des molécules carbonées à double liaison (*en bleu*) ; un composé carbonyle, comportant une double liaison entre un atome de carbone et un d'oxygène (*en vert*) ; le triméthylsilyl azide $(\text{CH}_3)_3\text{SiN}_3$, noté TMSN_3 (*en jaune*) ; enfin, le réactif d'Umemoto qui apporte le groupe trifluorométhyle (*en rouge*). La spirale découpée brouille les cartes et, en apportant une dynamique à l'œuvre, renvoie à la réaction elle-même. Quelle est-elle ?

Grâce au photocatalyseur, ici le $[\text{Ru}(\text{bpy})_3(\text{PF}_6)_2]$, le rouge et le bleu s'associent, le jaune et le vert font de même, et





les deux paires interagissent enfin pour former le composé recherché (*voir la formule ci-dessus*). Tous les réactifs sont réunis en une seule fois, la réaction étant dépendante d'une part de la quantité de chacun et, d'autre part, de leur réactivité.

Pour optimiser le résultat, on utilise une lumière adaptée au photocatalyseur, en l'occurrence du bleu pour le ruthénium (Ru). Les conditions requises sont plutôt douces, sans chauffage, et les produits utilisés sont peu toxiques (on utilisait auparavant des réactifs à base d'antimoine, beaucoup plus nocif). Au final, la production de déchets est limitée

au maximum et le coût énergétique notablement réduit.

Revenons à l'œuvre. L'artiste précise: «L'ensemble s'articule autour d'un nœud, défini comme le sujet de la peinture et comme une métaphore de la fusion des éléments sous l'effet de la réaction photocatalysée.» Divers systèmes graphiques, comme les hachures, les taches éparpillées, l'enchevêtrement de lignes fines... ajoutent un effet vibratoire empêchant l'œil d'accommoder et que d'aucuns, chimistes en premier lieu, pourraient rapprocher des vibrations qui agitent toute molécule, notamment lors d'une réaction.

Mais on ne doit pas y voir, Patrick Barrès insiste, une représentation figurative de ce qui se passe dans les récipients des chimistes. Tout n'est qu'évocation, suggestion... une vraie (al)chimie douce qui n'a rien contre quoi que ce soit. ■

G. Levitre et al., *Org. Lett.*, vol. 21(15), pp. 6005-6010, 2019.



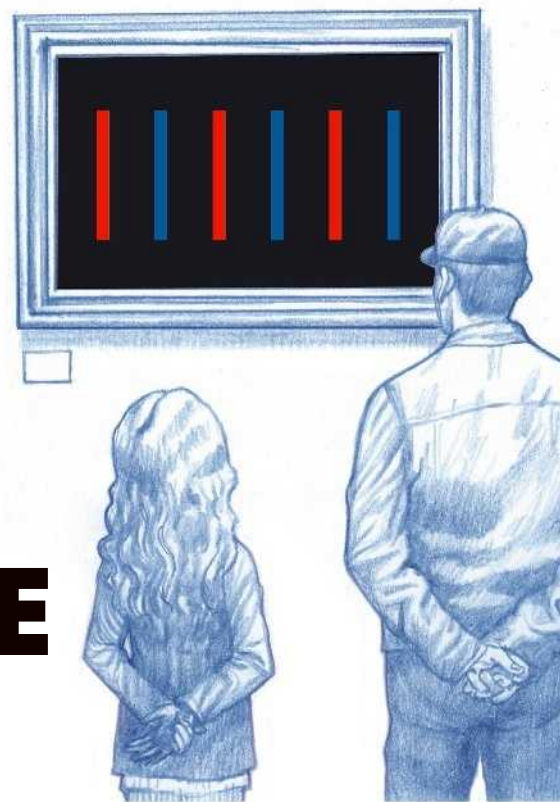
L'auteur a publié:
**Pollock, Turner, Van Gogh,
Vermeer et la science...**
(Belin, 2018)

LES AUTEURS



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

DE LA PROFONDEUR AVEC DU ROUGE ET DU BLEU



Certaines images colorées, bien que planes, sont perçues comme ayant du relief. L'effet trouve son explication dans les aberrations chromatiques et la physiologie de l'œil humain.

Goethe l'a mentionné dans son *Traité des couleurs* de 1810 : quand nous regardons certaines images composées de rouge et de bleu, les parties rouges semblent saillantes par rapport au plan de l'image, tandis que les parties bleues paraissent en creux (*voir l'illustration ci-dessus*). Cet effet a été utilisé comme procédé pour donner en peinture une impression de profondeur.

L'origine de l'effet est en grande partie physique et tient aux aberrations chromatiques de l'œil, semblables à celles des objectifs photographiques de mauvaise qualité : selon leur couleur, ou plus exactement leur longueur d'onde, les rayons

lumineux ne sont pas déviés de la même façon lorsqu'ils passent de l'air à l'intérieur de l'œil ou de l'objectif.

QUAND LA LUMIÈRE SE DISPERSE

Les aberrations chromatiques résultent de la dispersion de la lumière, observée par exemple lorsqu'un prisme de verre décompose un pinceau de lumière blanche. À chacune des interfaces air-verre, la composante bleue de la lumière est davantage déviée que sa composante rouge. Plus généralement, la lumière émerge du prisme en étant dispersée selon les couleurs de l'arc-en-ciel.

Pour comprendre ce phénomène et être quantitatif, nous avons besoin de

l'indice de réfraction de chaque milieu traversé, rapport entre la vitesse de la lumière dans le vide et la vitesse de la lumière dans le milieu. Ce nombre caractérise l'intensité de l'interaction de la lumière avec le milieu et dépend de la longueur d'onde lumineuse, et c'est de lui dont dépend directement l'angle de déviation des rayons.

L'air, peu dense, a un indice moyen de 1,0003, proche de 1, et son caractère dispersif est en conséquence faible. Tel n'est pas le cas du verre, comme l'illustre l'expérience avec le prisme, ou, pour notre sujet, de la cornée : l'indice moyen de celle-ci est 1,37, très proche de celui de l'eau (1,33), mais il varie de 0,012 entre la lumière rouge (0,65 micromètre