

COMMENT ÇA MARCHE

Les briques enchaînées de la blockchain

La technologie encore émergente de la *blockchain* se diffuse progressivement dans la chaîne de valeurs de l'assurance grâce à ses trois atouts : sa rapidité d'exécution, sa fiabilité et sa décentralisation.

1. UN REGISTRE DÉCENTRALISÉ

La *blockchain* est « un très grand cahier que, librement et gratuitement, tout le monde [peut] lire, sur lequel chacun [peut] écrire, mais qui [est] impossible à effacer et indestructible », explique le mathématicien Jean-Paul Delahaye. Comme le précise la définition macro de la *blockchain*, il s'agit d'un registre décentralisé et garanti identique, quelle que soit la source de consultation. À l'instar d'un document de travail collaboratif en ligne, chacun accède à la même information à un instant T. C'est ainsi que le *bitcoin* – cette monnaie numérique sans État – a été possible : il n'y a désormais plus besoin d'une source d'information centrale, comme une banque ou une administration, pour que les données soient fiables.

2. UN LIVRE COMPTABLE FIABLE ET SÉCURISÉ

La *blockchain* n'est donc pas qu'un registre de données décentralisé mais aussi un livre de compte sécurisé. La clef de cette sécurisation réside dans son nom composé des termes anglais *block* (ou brique), *chain* (enchaînée). Pour s'assurer que chaque donnée est à sa place, elle est enchaînée à la précédente.



À retenir

En France, les expérimentations de la *blockchain* concernent essentiellement les assurances incendie, accidents et risques divers, mais pas encore les assurances de personnes.

Chaque brique d'information porte non seulement sa propre identification mais a aussi gravé le nom de la brique précédente grâce à des méthodes de cryptographie, afin de garantir leur ordre d'apparition. L'enchaînement est traçable par ce code, au même titre que la parentalité peut être déduite de l'ADN d'un individu.

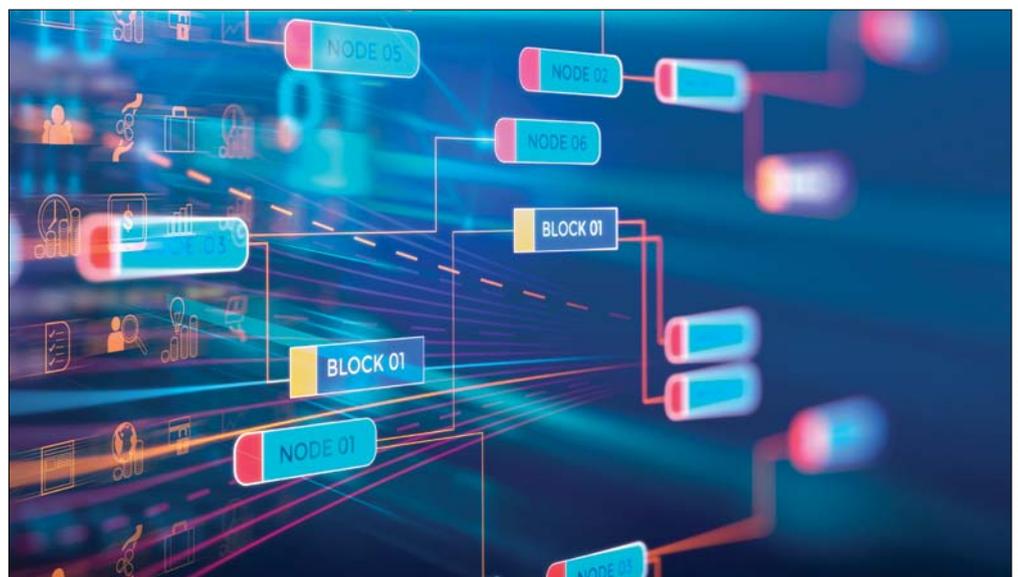
Pour garantir le registre, il faut aussi en sécuriser l'entrée. Il s'agit souvent de la preuve de travail (*proof of work*, PoW) qui consiste à demander à celui qui veut inscrire de nouvelles données de mettre à disposition de la communauté

une plus grande capacité de calcul informatique que celle dont il a besoin. En clair, il faut résoudre un problème mathématique, comme fonctionne le minage pour le *bitcoin*. Répondre correctement, c'est gagner son passage dans la *blockchain*.

3. UN CHAMP D'APPLICATION LARGE

Le potentiel d'utilisation de la *blockchain* peut être classé en trois catégories : les applications pour le transfert d'actifs, les applications en tant que registres (traçabilité des produits) et, enfin, les *smart contracts*. Il s'agit de programmes autonomes qui exécutent automatiquement les conditions et termes d'un contrat sans intervention humaine. Dans l'assurance, ces contrats intelligents sont capables, par exemple, de verser automatiquement une indemnisation proportionnelle au sinistre enregistré, d'assurer la traçabilité des œuvres d'art et des grands crus, de tenir une cartographie des risques à jour et disponible par tous les collaborateurs et prestataires habilités...

● MORGANE REMY



Dans la blockchain, chaque donnée est liée à la précédente.