La blockchain

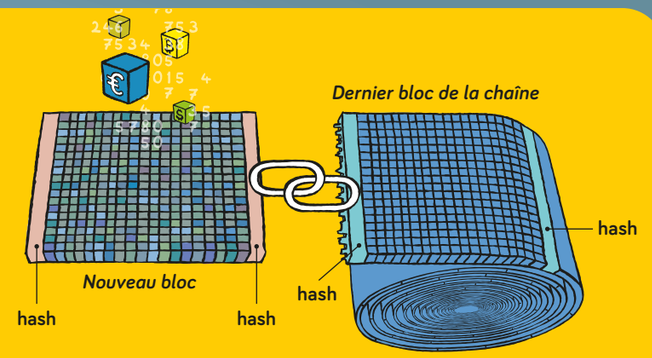
PRINCIPE

La *blockchain* (chaîne de blocs) est une technologie de stockage et de transmission d'informations, sécurisée par des outils cryptographiques, infalsifiable, transparente car distribuée chez tous ses utilisateurs et sans organe central de contrôle. C'est une sorte de registre mondial de données, qui contient l'historique de tous les échanges réalisés entre ses utilisateurs depuis sa création.

Qu'est-ce qu'une *blockchain* ?

C'est un enchaînement de blocs, un bloc étant une sorte de conteneur de données numériques.
Chaque bloc est identifié par un code cryptographique : le *hash*.
Les blocs s'enchaînent les uns après les autres pour former la chaîne de blocs, en respectant deux critères :

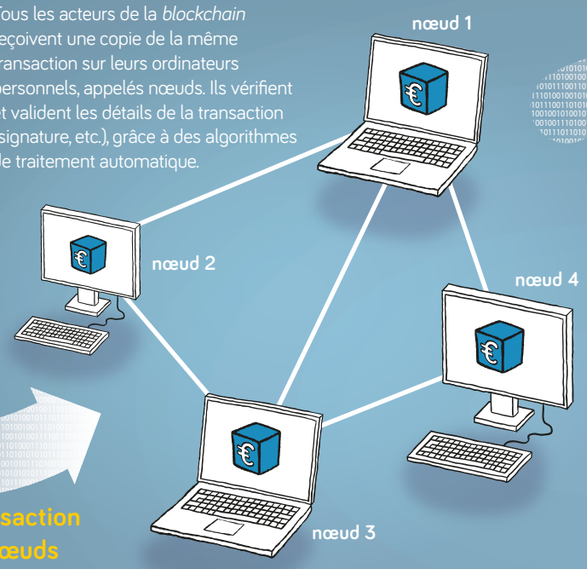
- un nouveau bloc ne peut s'enchaîner au dernier bloc de la chaîne que si son *hash* est « compatible » avec le *hash* précédent, à la manière de deux pièces de Lego© qui s'emboîtent ;
- l'ordre d'enchaînement est chronologique.



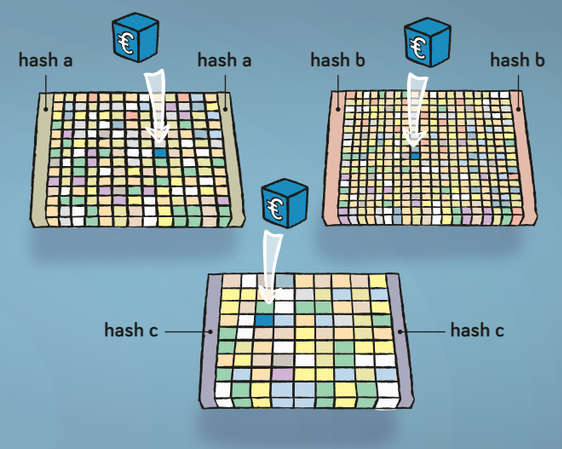
Transaction entre deux acteurs, A et B, authentifiée par la signature numérique de A (exemple : transfert d'argent, paiement, etc.).

Envoi de la transaction sur tous les nœuds du réseau de la *blockchain*

Tous les acteurs de la *blockchain* reçoivent une copie de la même transaction sur leurs ordinateurs personnels, appelés nœuds. Ils vérifient et valident les détails de la transaction (signature, etc.), grâce à des algorithmes de traitement automatique.



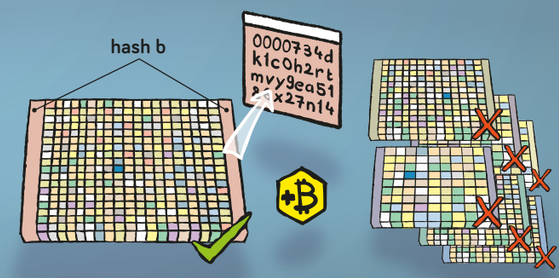
Insertion de la transaction dans un bloc



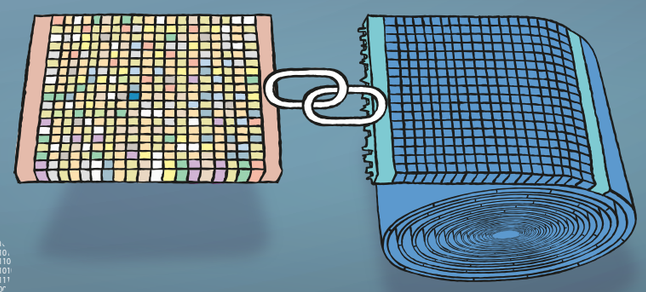
Étape de minage ou de preuve de travail (proof of work)
les transactions, une fois validées, sont regroupées dans des blocs. Ces blocs sont créés par des utilisateurs volontaires de la blockchain (appelés mineurs). Chaque bloc porte le marquage numérique (un code, appelé hash) issu du bloc précédent de la chaîne, qui atteste de sa validité, et un hash nouvellement créé. Cette opération (hashage) est réalisée par un algorithme, qui demande du temps et de la puissance de calcul.

Trouver le hash « magique »

L'objectif du hashage est de trouver le « bon » *hash*, c'est-à-dire la combinaison valide qui pourra s'enchaîner au dernier *hash* connu de la chaîne de blocs, à la manière d'un Lego©. Tous les mineurs sont en compétition pour trouver le *hash* « magique ». Le mineur ayant trouvé le bon *hash* est « récompensé » (paiement en cryptomonnaie par exemple).

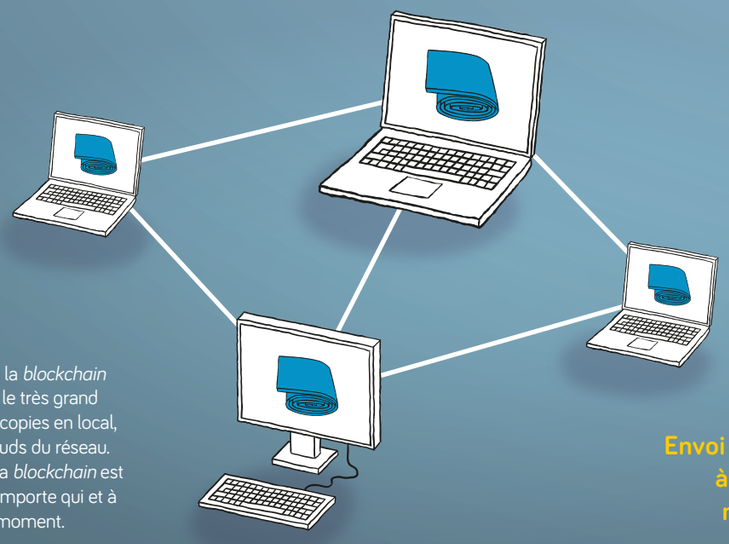


Mise à jour de la blockchain



Le nouveau bloc peut alors s'enchaîner au dernier bloc validé de la chaîne de manière immuable : une fois l'information inscrite dans la *blockchain*, il est quasi-impossible de la modifier ou de la supprimer. La *blockchain* est alors à jour.

Envoi de la *blockchain* à jour sur tous les nœuds du réseau



La pérennité de la *blockchain* est assurée par le très grand nombre de ses copies en local, sur tous les nœuds du réseau. L'ensemble de la *blockchain* est vérifiable par n'importe qui et à n'importe quel moment.

Les défis du CEA Septembre 2019 **N°239**
Sylvie Rivière et Aurélien Boudault (Infographie), avec la collaboration de **Sara Tucci (CEA-List)**.

TOUT S'EXPLIQUE

© Connecting Food

Grâce à Connecting Food, les consommateurs peuvent vérifier l'origine et la qualité des produits alimentaires.

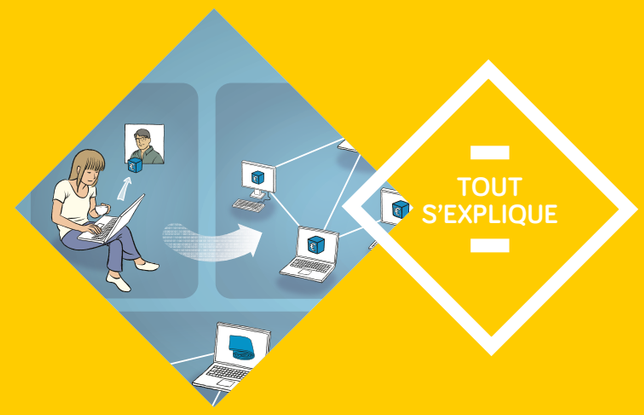
Un pôle de compétence dans les technologies *blockchain*

En 2018, le CEA-List crée un nouveau laboratoire entièrement dédié aux technologies *blockchain*. Ses équipes évaluent et proposent des algorithmes mis en œuvre au cœur des *blockchains*, qui garantissent la cohérence des données et leur inviolabilité ; étudient leurs propriétés (et hypothèses associées), les problématiques de passage à l'échelle, d'« interopérabilité » (c'est-à-dire de compatibilité entre différentes *blockchains* associées), l'analyse et le contrôle des menaces ; et accompagnent les acteurs industriels dans la mise en œuvre de solutions à base de *blockchain*, par exemple *via* la formalisation de *smart contratcs* dédiés, vérifiables.
Dernières actions en date : la mise au point d'une évolution de l'algorithme de consensus de la *blockchain* française Tezos, en collaboration avec Nomadic Labs ; et l'analyse de l'algorithme de Tendermint, une *blockchain* proposant une solution alternative au principe de la « preuve de travail » (*voir infographie*), beaucoup moins énergivore. L'étude a mis en évidence quelques faiblesses, rectifiées par les concepteurs avec l'aide du CEA-List.

Connecting Food trace et audite les produits alimentaires

La *start-up* Connecting Food, en partenariat avec le CEA-List, propose aux marques et aux consommateurs un nouveau service de traçabilité des produits alimentaires. Le principe ? Toutes les étapes de fabrication du produit, des fermes jusqu'aux supermarchés (origine, mode de production, intervenants…) sont enregistrées dans une *blockchain* afin de les rendre infalsifiables et consultables par tous. En cas de non-conformité d'un produit par rapport à son cahier des charges, l'acteur concerné (producteur, transformateur ou distributeur) est même alerté en temps réel ! À la clé : une réduction du gaspillage et des rappels-produits, et une confiance restaurée des consommateurs. La marque peut aussi décider d'appliquer un QR code « Connecting Food » sur son produit, donnant ainsi au client un accès à l'ensemble du parcours du produit, par simple scan *via* un smartphone. Petit plus : la *blockchain* utilisée fonctionne sans minage, et consomme donc beaucoup moins d'énergie !

les défis du cea 239



TOUT S'EXPLIQUE

La blockchain

Voilà déjà plus de 10 ans que la *blockchain* – le support logiciel de la monnaie numérique *Bitcoin* – est née.
Elle fait aujourd'hui partie des technologies à suivre dans les années à venir, tant ses applications sont nombreuses.
Tous les domaines pour lesquels il est nécessaire d'assurer une traçabilité indélébile sont susceptibles d'en bénéficier.

ENJEUX

La technologie *blockchain* pourrait bien révolutionner plusieurs secteurs de l'économie. Les champs d'exploitation aujourd'hui envisagés sont immenses : banque (garantie de transaction), assurance (automatisation du traitement des sinistres), notariat (garantie et suivi de transfert de propriétés), transport, commerce (lutte contre le vol et la contrefaçon), musique (rémunération automatique des auteurs-compositeurs *via* les plateformes de *streaming*), industrie au sens large (certification, chaîne logistique, suivi de pièces détachées, détection de fraude…).
Trois domaines d'utilisation sont pressentis :

- Le transfert d'actifs : argent, actions, obligations… ;
- Les applications en tant que registre infalsifiable et consultable par tous, qui permettent d'assurer une traçabilité de toutes sortes de produits ;
- Les *smart contracts* : programmes autonomes exécutant automatiquement les conditions et termes d'un contrat, sans intervention humaine. Si telle condition est vérifiée, alors telle conséquence s'exécute. Exemple : des passagers automatiquement indemnisés lorsque leur vol est en retard, sans avoir besoin de remplir de formulaire ; ou une indemnité d'assurance automatiquement versée en cas de sinistre déclaré et vérifié.