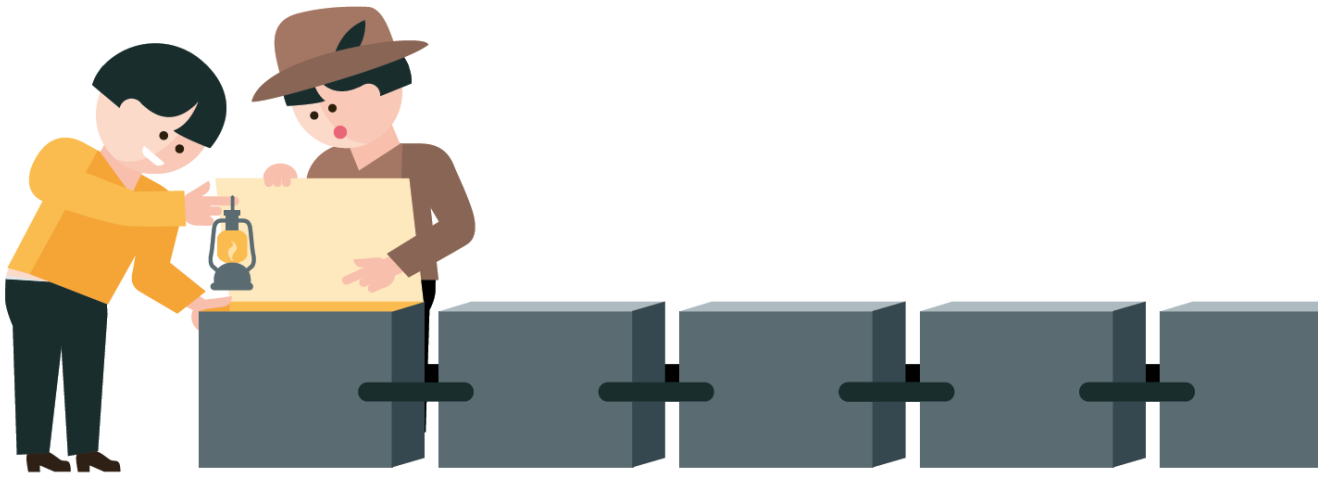

Maillons essentiels enchaînés

En règle générale, lorsqu'un objet de valeur change de main ou que des accords importants doivent être consignés dans un contrat, il faut qu'une autorité intervienne comme intermédiaire. Il peut s'agir d'un notaire qui légalise la transaction en question et certifie les signatures, ou d'une banque qui crée la monnaie, permettant d'effectuer les paiements et d'initier les flux financiers.

La technologie blockchain pourrait bientôt rendre ces intermédiaires superflus car elle crée un lien direct entre toutes les personnes ou institutions appartenant à un même réseau – et ce d'une manière qui rend impossible toute manipulation ou falsification.

Les échanges commerciaux, transactions ou encore rapports de propriété et accords dont l'enregistrement nécessitait jusqu'ici l'intervention d'une autorité – comme un registre foncier – ne sont plus centralisés dans une seule base de données, mais stockés de manière décentralisée sur plusieurs ordinateurs du réseau. Plus le réseau compte de nœuds, c'est-à-dire de participantes et participants, plus il est fiable et protégé contre les manipulations.

Des services financiers au commerce de l'électricité

Parmi toutes les applications de la blockchain, la plus connue est la monnaie virtuelle Bitcoin. Mais paradoxalement, il est peu probable que la technologie blockchain connaisse un réel succès à long terme dans le domaine des devises. Les échanges non réglementés, combinés à une masse monétaire stable, conduisent à des fluctuations extrêmes de prix comme celles qui se sont produites à répétition avec le Bitcoin. Or, pour être incontestée, une monnaie a besoin d'une certaine stabilité.

Dans les services financiers, en revanche, la blockchain pourrait ouvrir la voie à des processus moins coûteux et plus rapides. En effet, elle permet de vérifier les rapports de propriété et d'origine en toute transparence sans dépendre de la lourdeur bureaucratique d'un service de renseignements centralisé.

Un bel avenir est prédit à la blockchain dans ce qu'on appelle les « contrats intelligents » (en anglais, smart contracts). Il s'agit de contrats numériques qui se réalisent d'eux-mêmes, où une transaction est automatiquement déclenchée par un algorithme au moment où certains événements préalablement définis se produisent, avant d'être validée et stockée dans un bloc. Toute surveillance par un être humain devient superflue. Les contrats intelligents peuvent être utiles dans des contextes très différents, comme lorsque plusieurs propriétaires de biens immobiliers dont le toit est équipé de panneaux solaires échangent de l'électricité entre eux. Un « smart contract » peut également se concevoir pour qu'une prime d'assurance automobile augmente automatiquement si la boîte noire installée dans le véhicule enregistre une violation répétée des règles de circulation.

La Suisse est en bonne position pour profiter de ces innovations potentielles : son cadre réglementaire libéral, qui a déjà attiré un grand nombre de pionniers de la blockchain, augmente ses chances d'être choisie comme juridiction pour de nombreux contrats intelligents.

Obstacles et limitations

La technologie de la blockchain en elle-même impose certaines limites techniques à son développement puisque qu'une « chaîne » ne peut pas croître à l'infini. En effet, le nombre de données augmente à chaque bloc, et le réseau décentralisé devient de ce fait plus lent. C'est pourquoi les

fichiers volumineux tels que les vidéos ou les images ne peuvent pas être stockés directement dans la blockchain.

De plus, une fois définis, les contrats intelligents sont relativement peu flexibles : ils ne peuvent pas s'adapter aux changements de circonstances tels qu'il s'en produit dans la vie réelle et où un droit peut expirer ou un objet peut se casser. Pour tenir compte de ces variations, les contrats intelligents devraient attribuer des droits de modification à des tiers tout en évitant de créer des hiérarchies indésirables.

Si transparence et immuabilité sont les atouts de la blockchain, elles constituent en même temps son point faible. En effet, elles font obstacle au droit à l'oubli tel que le prévoit la loi sur la protection des données.

Outre les écueils d'ordre technique, il existe également des obstacles d'ordre psychologique. En effet, pour tirer parti de cette nouvelle technologie, les procédures et habitudes établies doivent être abandonnées et remplacées. La plupart des gens ont tendance à faire confiance à un système activement contrôlé par une seule instance plutôt qu'à un réseau où, au bout du compte, la responsabilité incombe à tout le monde et à personne en même temps.

Un tour d'horizon

Dans son étude « Blockchain : Capabilities, Economic Viability and the Socio-Technical Environment » et à la lumière de 12 études de cas, TA-SWISS montre où le recours à la blockchain est judicieux et où il ne l'est pas. Dans un deuxième temps, la blockchain, sa genèse et la façon dont elle est perçue sont placées dans un contexte sociologique et culturel. Les autrices et auteurs examinent ensuite comment l'opacité supposée du système pour le grand public impacte le discours social autour de la blockchain, et qui a intérêt à entretenir un certain battage médiatique à cet égard. Cette étude apporte une valeur ajoutée du fait qu'elle adopte une vision d'ensemble de la blockchain, qu'elle l'inscrit dans son contexte international et qu'elle donne une assise factuelle aux débats et à l'enthousiasme qu'elle suscite. Une chose est sûre : le potentiel de cette technologie est considérable. Mais il manque encore une « application tueuse » (killer app) qui lui permette véritablement de percer.

Comment fonctionne la blockchain ?

À l'origine de toute chaîne de blocs se trouve le « bloc de création » (en anglais, genesis block). Celui-ci contient le protocole dit de consensus et définit les règles de base. Viennent ensuite les blocs contenant les transactions stockées. Les blocs sont reliés entre eux par une empreinte numérique, appelée valeur de hachage (en anglais, hash value). Cette valeur est calculée à partir des entrées du bloc précédent et enregistrée dans le nouveau bloc. Même la plus petite modification des entrées du bloc précédent entraînera une valeur de hachage complètement différente. Cela permet de détecter facilement toute manipulation ultérieure.

Lorsque deux parties conviennent d'une transaction ou de tout autre arrangement contraignant, elles déterminent d'abord les paramètres clés : quel en est l'objet, qui obtient quoi et à quelles conditions ? Un nœud du réseau (en anglais, node), c'est-à-dire une personne participant à la blockchain, vérifie ensuite si la transaction est fondamentalement valide et en particulier si l'expéditeur dispose de suffisamment de monnaie électronique sur son compte. Une telle transaction est ensuite combinée à d'autres transactions pour former un bloc. C'est là qu'entrent en jeu les « mineurs » (en anglais, miners), les chercheurs d'or numériques.

Les mineurs collectent les transactions connectées des nœuds du réseau et en combinent plusieurs dans un bloc. Pour que celui-ci devienne le nouveau bloc valide, il doit remplir une condition : sa valeur de hachage doit être inférieure à un nombre donné. Pour trouver une valeur appropriée, les mineurs doivent répéter le calcul avec des valeurs initiales à chaque fois légèrement différentes. Cette procédure, appelée preuve de travail (en anglais, proof of work), nécessite une puissance de calcul extrême. Les mineurs y travaillent avec des milliers d'ordinateurs en même temps. Dans le cas du Bitcoin, par exemple, près de deux cent mille milliards de valeurs de hachage sont calculées chaque seconde dans le monde. Celui qui trouve le plus rapidement une valeur correspondante ajoute son nouveau bloc à la chaîne existante. La récompense consiste en de nouveaux Bitcoins et en l'affranchissement numérique dû par les utilisatrices et utilisateurs pour leurs transactions.

Informations complémentaires

- Étude complète « Blockchain: Capabilities, Economic Viability, and the Socio-Technical Environment » : https://vdf.ch/blockchain-capabilities-economic-viability-and-the-socio-technical-environment-e-book.html
- Synthèse de l'étude « Confiance programmée : Chances et risques de la technologie blockchain » : www.zenodo.org/record/3922035
- Pour plus d'informations sur le projet, rendez-vous sur notre site Internet : www.ta-swiss.ch/blockchain

TA-SWISS
Fondation pour l'évaluation des choix technologiques
Brunngasse 36
3011 Berne

www.ta-swiss.ch

membre des
académies suisses des sciences