fonctionnement en parallèle des programmes est une forme de gâchis, mais avec les puissances de calcul dont nous disposons, c'est sans grande importance si cela assure la sécurité de l'ensemble et autorise des applications d'un type nouveau. Chaque machine présente sur le réseau et participant à l'exécution des programmes augmente la sécurité et la fiabilité de l'ensemble, qui devient alors quasiment indestructible.

Blockchain et bitcoin

La mémoire de cet ordinateur virtuel est ce qu'on nomme la blockchain (ou chaîne de blocs). C'est un fichier informatique présent en chaque nœud du réseau et qui évolue en parallèle sous la forme de multiples copies identiques. Cette recopie au sein de dizaines de machines réparties dans le monde explique la solidité de la construction. Qu'importe que certaines machines du réseau tombent en panne, ou même que des secteurs entiers du réseau se trouvent momentanément isolés : les machines présentes continueront de faire fonctionner l'ordinateur-monde dont la mémoire, la blockchain, poursuivra son évolution, prête à se recopier sur les machines un moment défaillantes ou à s'installer sur des machines nouvelles.

Personne ne peut effacer ou modifier cette mémoire commune partagée. Son contenu évolue par ajout de pages ou blocs chaînés, par des procédés assurant le repérage d'une modification intempestive et l'empêchant.

Le bitcoin, inventé pour disposer d'une monnaie sans autorité centrale d'émission et de régulation, a été la première mise en application de cette idée d'une mémoire partagée, multipliée, protégée, dont l'évolution est contrôlée par un réseau pair à pair et qui ne se fait que par ajout. Son inventeur, Satoshi Nakamoto, n'a peut-être pas envisagé que son idée était généralisable.

Les opérations autorisées par l'ordinateur à blockchain du réseau bitcoin ne sont cependant que des opérations élémentaires de déplacement d'argent d'un compte vers un autre. Ces transactions exécutées par l'ordinateur-monde du bitcoin rendent disponible toute somme d'argent en bitcoins, qui passe

Un peu de vocabulaire...

RÉSEAU PAIR À PAIR – Système d'échange de messages entre ordinateurs connectés leur permettant d'émettre et de recevoir des informations sur un pied d'égalité. Ces échanges autorisent leur synchronisation et l'utilisation d'une même mémoire recopiée à l'identique dans chacun d'eux.

BLOCKCHAIN (CHAÎNE DE BLOCS) – Fichier partagé sur un réseau pair à pair où par exemple sont inscrites la totalité des transactions entre des comptes, ce qui autorise le calcul du solde de chaque compte. Dans le cas de la blockchain d'Ethereum, des informations sur chaque programme d'Ethereum sont inscrites dans ce fichier dont chaque nœud principal du réseau détient une copie. Cela permet à chaque machine du réseau d'exécuter ces programmes en parallèle et à l'identique. La blockchain évolue par ajout périodique de pages, ou blocs.

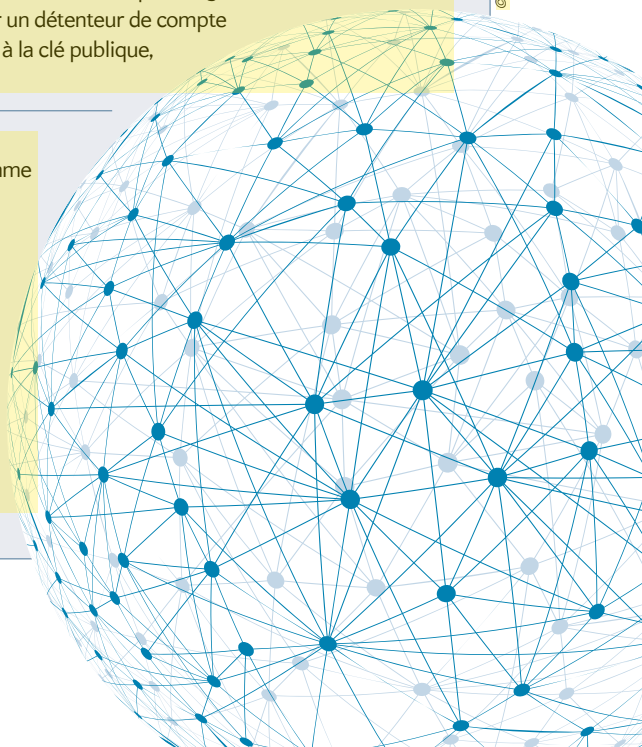
ORDINATEUR À BLOCKCHAIN OU ORDINATEUR-MONDE – L'ensemble des ordinateurs d'un réseau pair à pair partageant une blockchain sur laquelle sont présents des programmes ainsi que les informations sur l'état de leurs calculs. Cet ensemble constitue un ordinateur virtuel délocalisé et indestructible où chaque ordinateur du réseau contrôle tous les autres et est contrôlé par eux. Grâce à une telle structure, les pannes et les fraudes sont presque impossibles.

MONNAIE CRYPTOGRAPHIQUE – Monnaie créée par un ordinateur à blockchain lorsque la blockchain contient des informations sur les comptes des utilisateurs et sur les transactions faites entre comptes. La plus importante (10 milliards d'euros) est le bitcoin, la seconde est l'éther (1 milliard d'euros) du réseau Ethereum.

SMART-CONTRACT OU CONTRAT INTELLIGENT – Programme d'un ordinateur à blockchain. Ce terme est à éviter, car ces programmes exécutés par chacun des ordinateurs du réseau ne sont en rien des contrats au sens juridique.

TRANSACTION, CLÉ PRIVÉE, CLÉ PUBLIQUE – Si un ordinateur à blockchain gère des transactions, celles-ci s'opèrent entre comptes, chacun possédant deux clés. La première, assimilable à un numéro de compte, est publique. La seconde, privée, permet à celui qui la connaît (celui qui a créé le compte) d'agir sur le compte. Les transactions faites par un détenteur de compte sont vues par tous et peuvent, grâce à la clé publique, être contrôlées et validées par tous.

ORGANISATION AUTONOME DÉCENTRALISÉE (DAO) – Programme fonctionnant grâce à un réseau pair à pair, qu'il est impossible d'arrêter et qui, du fait de sa fiabilité et des protections cryptographiques dont il bénéficie, crée de la confiance entre personnes utilisant le programme. Le système du bitcoin et celui d'Ethereum sont des DAO. Les programmes déposés sur la blockchain d'Ethereum (sauf s'ils sont trop simples) sont des DAO.



© Vinko93/shutterstock.com