LOGIQUE & CALCUL

Du bitcoin à Ethereum : l'ordinateur-monde

Les « organisations autonomes décentralisées » sont des programmes indestructibles fonctionnant sans que personne ne puisse en prendre le contrôle. Elles ouvrent des perspectives inattendues, pour le meilleur et pour le pire.

Jean-Paul DELAHAYE

On attribue à l'ingénieur mathématicien Héron d'Alexandrie, au I^er^ siècle de notre ère, l'invention d'une machine à distribuer de l'eau qu'on mettait en marche en introduisant des pièces de monnaie. D'autres distributeurs automatiques ont été exploités dans les tavernes anglaises au XVII^e^ siècle pour vendre du tabac. Aujourd'hui, on trouve des versions de plus en plus perfectionnées et variées de ce type de dispositifs. Il y a la machine à café capable de prendre une dose de grains, de la moudre, de chauffer l'eau nécessaire et de préparer en quelques secondes la boisson que vous avez choisie dans une longue liste et payée avec des piécettes. Il y a les distributeurs de sachets de bonbons, de barres chocolatées, etc. Ajoutons les machines à distribuer des billets, les parcmètres, les bandits manchots des casinos, les flippers des bars. Et, plus récemment, les vélos et autos que vous louez dans la rue sans intermédiaire humain.

L'idée est de concevoir et fabriquer un dispositif qui travaillera tout seul. La machine offre un contrat implicite au client potentiel : ce dernier paye, le mécanisme fonctionne et le client reçoit son dû : un produit, une boule lancée sur le plan incliné du flipper, une voiture en prêt, etc.

Puisque l'automate est un objet matériel coûteux à construire, il a un propriétaire qui en effectue la maintenance et renouvelle les produits de base nécessaires (eau, doses de café, sachets de bonbons, etc.). C'est lui qui réserve l'emplacement où est déposé le dispositif ; c'est lui qui en tire du profit et qui est victime s'il y a vol ou dégradation.

L'informatique vient d'inventer une version perfectionnée de ces « entreprises autonomes automatiques » qui, jusqu'à présent, n'étaient que partiellement autonomes et imparfaitement automatiques, puisque l'humain devait intervenir pour maintenir le système en marche et qu'à chaque instant il pouvait en interrompre le fonctionnement.

Les descendants actuels de la machine d'Héron d'Alexandrie ont des propriétés inattendues. Ils sont décentralisés, car situés partout sur le réseau, et ne sont pas nécessairement au service d'un propriétaire identifié. Ils peuvent fonctionner selon des procédures sans aucune limite de complexité ou presque, recevoir des informations variées et se comporter en fonction de ces dernières. Ils possèdent et dépensent de l'argent. Ils sont quasiment indestructibles et inviolables, car leur bonne marche s'appuie sur des protections cryptographiques et sur la copie en multiples exemplaires de leur mémoire. Une fois lancés, leur autonomie et leur indépendance sont aussi parfaites que possible, même si aujourd'hui, certaines étapes restent à franchir entre le rêve et la réalité. On les nomme organisations autonomes décentralisées ou DAO (pour *Decentralized Autonomous Organization*), sigle commode qui s'est imposé.

Tout provient des monnaies cryptographiques, dont le *bitcoin* créé en 2009 est de loin la principale, et de la technologie sur laquelle elles s'appuient : les réseaux pair à pair et la *blockchain*.

L'idée centrale est de créer un ordinateur virtuel, un ordinateur-monde, dont le fonctionnement ne s'appuie pas sur une machine particulière, mais sur une multitude de machines indépendantes, liées en un réseau robuste.

Un système disséminé et permanent

Ce réseau dit pair à pair, car aucun nœud central ne le dirige et ne le contrôle, assure que les programmes de l'ordinateur-monde continuent de fonctionner quoi qu'il arrive à l'un de ses composants, voire à plusieurs d'entre eux. Aucun n'est indispensable, tous communiquent sur un pied d'égalité. Ils se suppléent, faisant fonctionner les mêmes instructions et gérant une mémoire collective recopiée partout à l'identique, la blockchain. Ils s'occupent aussi à chaque instant de créer un consensus sur les informations qu'ils détiennent.

Ce réseau est conçu pour que, une fois en marche, l'ordinateur-monde auquel il donne vie ne s'arrête plus et ne puisse être pris en main par personne. Les règles fixées au départ pour ses programmes s'exécutent sur toutes les machines du réseau sans que quiconque puisse intervenir. Le

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.

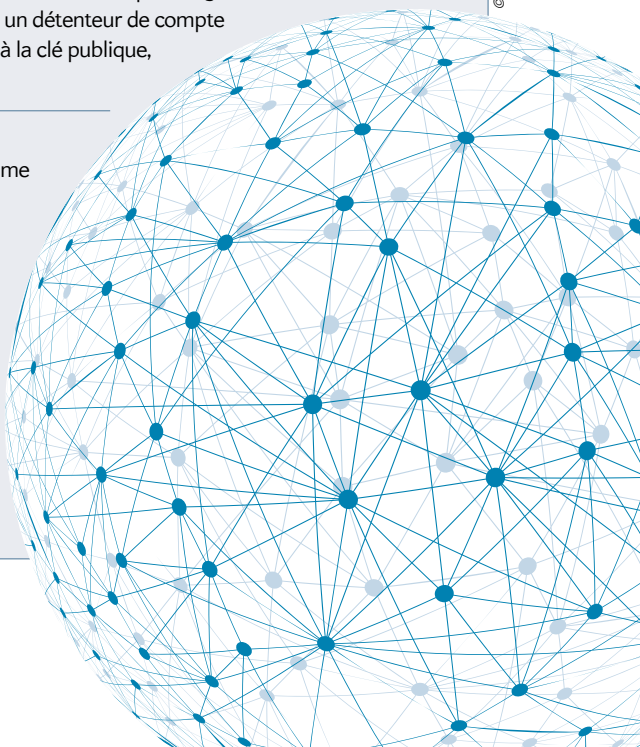
ORDINATEUR À BLOCKCHAIN OU ORDINATEUR-MONDE – L'ensemble des ordinateurs d'un réseau pair à pair partageant une blockchain sur laquelle sont présents des programmes ainsi que les informations sur l'état de leurs calculs. Cet ensemble constitue un ordinateur virtuel délocalisé et indestructible où chaque 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