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