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.

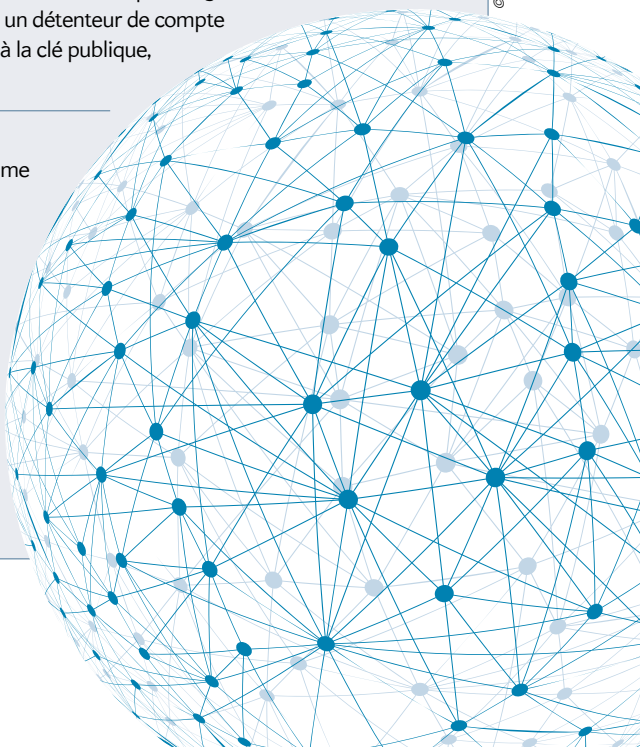
ORDINATEUR À BLOCKCHAIN OU ORDINATEUR-MONDE – L'ensemble des ordinateurs d'un réseau pair à pair partageant une blockchain sur laquelle sont présents des programmes ainsi que les informations sur l'état de leurs calculs. Cet ensemble constitue un ordinateur virtuel délocalisé et indestructible où chaque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

Quelques repères chronologiques


Vitalik Buterin

- **Janvier 2009** La monnaie cryptographique bitcoin est lancée par la mise en fonctionnement du réseau bitcoin. Son créateur se dénomme Satoshi Nakamoto, mais reste inconnu. Le réseau bitcoin est la première DAO importante.
- **Fin 2013** Un jeune Russo-Canadien, Vitalik Buterin, conçoit le projet Ethereum.
- **Janvier 2014** Vitalik Buterin annonce le projet Ethereum et commence à y travailler avec une petite équipe de développeurs.
- **Juillet 2014** La fondation Ethereum vend durant 42 jours des ethers avant même la mise en fonctionnement du réseau Ethereum. Dix-huit millions de dollars sont tirés de cette vente.
- **Juillet 2015** Une plateforme de test est rendue disponible et permet de se faire une idée de l'ordinateur-monde conçu par Vitalik Buterin, qui réside désormais en Suisse. Le 30 juillet, la blockchain d'Ethereum se met à fonctionner.
- **Janvier 2016** Onze banques, dont le Crédit Suisse et HSBC, entreprennent des essais avec une plateforme de test d'Ethereum. Des start-up dont l'activité tourne autour d'Ethereum naissent et lèvent des fonds.
- **Mars 2016** Les ethers en circulation valent 1 milliard de dollars (les bitcoins, eux, 10 milliards).
- **Mai 2016** Le programme intitulé The DAO, qui est une organisation autonome décentralisée sur la blockchain d'Ethereum, collecte des fonds pour aider les investissements liés à Ethereum. Il réussit à collecter plus de 160 millions de dollars.
- **Juin 2016** Le programme The DAO est victime d'une attaque, rendue possible par une erreur dans son programme. Une somme d'environ 50 millions de dollars est déplacée. Elle reste toutefois bloquée sur la blockchain, ce qui donne le temps de trouver une solution pour éviter que le vol devienne effectif.
- **Juillet 2016** L'annulation de certaines opérations de la blockchain d'Ethereum règle le problème de l'attaque de juin, mais donne lieu à la création d'une nouvelle version d'Ethereum du fait d'un désaccord entre utilisateurs. La leçon est sévère : il faut éviter que de trop fortes sommes soient déposées dans un seul programme de la blockchain Ethereum et, surtout, il faut utiliser des méthodes rigoureuses de développement pour éviter les bugs. Le cours de l'ether n'est que peu affecté par cette attaque qui n'a pas concerné directement l'ordinateur-monde Ethereum, mais seulement une DAO construite (maladroitement !) sur lui.

Selon le chercheur et développeur Travis Patron, « l'une des caractéristiques fondamentales de la société du XXIe siècle est que le rôle de l'employé est tenu par des machines aussi bien que par des humains. Avec le bitcoin, on a l'un des premiers exemples de ce type de fonctionnement. Les mineurs du réseau bitcoin sont des employés, analogues aux humains des entreprises traditionnelles. Ethereum porte cette idée plus loin. Le rôle du client, actuellement réservé aux humains, pourra tout aussi bien être tenu par des machines… Ethereum facilitera une économie de dispositifs interconnectés où les machines transmettent de l'argent et des données plus efficacement que ne le font les humains. Les entreprises qui négligeront ces possibilités le paieront cher, car elles n'utiliseront pas ces nouveaux systèmes de communication et d'action qui simplifient le monde ancien en éliminant la médiation de tiers inutiles… »

sans quasiment aucun coût d'un point du globe à un autre. Un bitcoin (le mot désigne à la fois le réseau et l'unité monétaire associée) vaut aujourd'hui environ 600 euros et la totalité des bitcoins atteint 10 milliards d'euros. La fiabilité de l'ordinateur virtuel du bitcoin, attestée par bientôt huit ans de bon fonctionnement, explique la confiance que les utilisateurs ont dans cette monnaie et en cette organisation autonome décentralisée. En détenant l'historique de toutes les transactions, la blockchain du bitcoin permet de connaître le contenu de chaque compte. Des opérations un peu plus complexes que les simples transactions sont permises pour cette DAO, mais sa capacité est réduite à des séries finies de transactions.

Le réseau des bitcoins est bien une DAO dont la blockchain est recopiée environ 6 000 fois (en septembre 2016) sur toute la Terre. Pour le détruire, il faudrait réussir à interrompre le réseau partout à la fois. Ce n'est pas impossible, mais très improbable.

Cette autonomie de la DAO du bitcoin a réussi (contre toute attente) à émettre une monnaie que personne ne contrôle et qui, du fait des diverses protections présentes dans ses mécanismes, a maintenant convaincu des millions d'utilisateurs. C'est une aventure fantastique, même si quelques inquiétudes et difficultés persistent !

Ethereum, un outil général

Le premier projet d'envergure mis en place pour reprendre et généraliser l'idée de l'ordinateur à chaînes de blocs du bitcoin se nomme Ethereum. C'est lui-même une DAO comme le réseau bitcoin, mais c'est surtout un outil qui permet de créer facilement de nouvelles DAO.

Ethereum a été annoncé le 25 janvier 2014 par Vitalik Buterin. Né à Moscou en 1994, ce surdoué de l'informatique a abandonné ses études à l'âge de 20 ans pour participer à l'effervescence résultant des premiers succès du bitcoin et des entreprises qui naissaient dans son sillage. Il est l'un des acteurs principaux de cette révolution qui complète et amplifie celle des monnaies cryptographiques.

L'idée d'Ethereum est de faire fonctionner un ordinateur à blockchain comme celui du bitcoin, mais sans en limiter les opérations de base et en autorisant donc d'y exécuter des programmes aussi généraux que possible, écrits dans un langage de programmation qualifié de Turing-complet (permettant de calculer toute fonction calculable par algorithme), ce qui permet de créer aisément de nouvelles DAO. Non seulement la blockchain reçoit et accumule des transactions pour la monnaie nommée ether dont elle assure la gestion des comptes, mais elle reçoit aussi des programmes de toutes sortes (appelés parfois contrats-intelligents ou smart-contracts, termes que nous éviterons, car il ne s'agit en rien de contrats au sens juridique) qui, une fois déposés sur la blockchain, y resteront toujours.

L'ether, dont nous verrons qu'il joue un rôle fondamental dans le fonctionnement de la blockchain Ethereum, valait en septembre 2016 une douzaine d'euros, ce qui donne un total d'environ 1 milliard d'euros en circulation sous la forme d'ethers. C'est la seconde monnaie cryptographique en importance derrière le bitcoin. Si l'ether se révèle aussi robuste que le bitcoin, il pourrait à terme le rattraper ou même le supplanter. Donnons un exemple de DAO construite sur la blockchain d'Ethereum.

Une loterie de fête foraine est un mécanisme simple qui reçoit de l'argent des joueurs et qui, après un tirage au hasard en faisant tourner la roue, prend l'argent des perdants et redistribue de l'argent aux gagnants, s'il y en a. Tout se déroule en fonction de règles fixées à l'avance.

Les opérations consistant à recevoir de l'argent, à effectuer un tirage au hasard, à redistribuer certaines sommes aux gagnants, sont parfaitement automatisables. Il leur correspond un programme qu'on peut déposer sur la blockchain d'Ethereum et qui s'exécutera automatiquement quand des joueurs se présenteront. On peut même prévoir que celui qui crée le programme prélève une partie de l'argent misé. Cette commission, par exemple de 1 %, sera versée automatiquement sur un compte particulier dont seul le créateur du programme détiendra les clés permettant d'en profiter. Les avantages d'une telle organisation autonome décentralisée de type loterie sur la loterie classique à roue sont nombreux :

– pas besoin d'être au même endroit que la roue de la loterie pour jouer. Quiconque a accès au réseau pair à pair d'Ethereum peut miser, et ce réseau est accessible partout dans le monde grâce à Internet ;

– tout joueur peut connaître le programme qui simule la loterie, car ce qui est présent sur la blockchain est public. Il peut donc vérifier que le tirage au sort est équitable et que le calcul de la redistribution de l'argent misé est conforme à ce qui est annoncé. Pas besoin donc de faire confiance à l'organisateur, qui ne peut rien cacher et qui ne contrôle pas l'ensemble des machines faisant fonctionner le programme de loterie sur lequel il n'a aucun pouvoir, une fois ce programme déposé ;

Les qualités d'une organisation autonome décentralisée : transparence, sûreté et vérifiabilité

– après coup, tout le monde voit tous les déplacements d'argent qui ont été effectués, dont les traces resteront toujours présentes sur la blockchain, permettant l'analyse après coup de tout ce que fait la loterie ;

– autre avantage d'une loterie Ethereum, on est certain qu'une fois en marche l'organisation initiale, celui qui l'a programmée ne la modifiera pas et n'interrompra pas son fonctionnement. En particulier, garder les sommes misées et empêcher la distribution des gains aux gagnants est impossible. Pas de filou qui part avec la caisse, comme cela se pratique parfois pour les sites internet de jeu… ou dans la vraie vie.

Voici donc les qualités d'une organisation autonome décentralisée de type loterie :

1) transparence : tout est public ;

2) sûreté absolue : l'ordinateur qui organise les tirages n'est pas une machine isolée aux mains d'un inconnu, mais le réseau composé de centaines de machines qui se contrôlent mutuellement et se suppléent en cas de panne ;

3) possibilité d'auditer et de vérifier l'équité et la correction du fonctionnement dont tout le passé subsiste indéfiniment.

Le mode de fonctionnement de l'ordinateur-monde crée ainsi de la confiance, même entre partenaires qui ne se sont jamais rencontrés, et cela sans le contrôle d'aucune autorité centrale et sans avoir à faire appel à un tiers de confiance. Le stockage multiple de la blockchain rassure les acteurs, même éloignés. Ils peuvent se faire confiance car leurs échanges sont publics, surveillés, ineffaçables et suivent des règles inamovibles, qui s'appliquent sans exception.

Une multitude d'applications où de l'argent circule entre les acteurs sans recours à un tiers de confiance deviennent envisageables. Des jeux bien plus complexes qu'une loterie ont ainsi été déposés sur la blockchain d'Ethereum. On a aussi créé des systèmes gérant des outils financiers et des engagements divers. Bien évidemment, à part l'ether, d'autres monnaies cryptographiques fondées sur Ethereum ont été créées. L'option offerte aux programmes d'aller rechercher des informations sur Internet et de faire dépendre leur comportement de ce qu'ils y trouvent permet d'organiser des paris sportifs ou de toute nature. Sans surprise encore, des systèmes de vote parfaitement contrôlables et fiables ont été programmés et on a même envisagé d'organiser les élections en Ukraine avec ce programme.

Résistance aux attaques

Un autre type d'applications en cours de développement permettrait de gérer des serrures connectées au réseau par le biais d'un programme sur la blockchain Ethereum. Une fois la serrure installée à l'entrée de l'appartement que vous proposez à la location, tout se fera automatiquement sans que vous ayez à intervenir. Le locataire intéressé paiera par exemple un mois de location, et obtiendra en échange un code lui permettant, pendant la période concernée, d'ouvrir la serrure de l'appartement. Le code cessera d'être actif à l'issue de ce mois. Le

paiement de la location, le transfert vers votre compte de l'argent reçu, la détermination du code pour l'ouverture de la porte, sa mise en fonctionnement pendant un mois, tout cela sera géré automatiquement par le programme déposé sur la blockchain de l'ordinateur-monde. Personne ne pourra tricher avec ses engagements, ni le propriétaire ni le locataire. (Pour d'autres applications, voir http://dapps.ethercasts.com.)

Si l'utilisation des programmes sur la blockchain n'exigeait aucune contrepartie, on pourrait y faire fonctionner un programme qui tourne indéfiniment et consomme la puissance des ordinateurs du réseau. Sans moyen de freiner cette consommation de puissance, on arriverait à saturation et il serait facile de mettre en panne le réseau tout entier par l'introduction délibérée de programmes exécutant des calculs excessivement gourmands en puissance qu'on ferait fonctionner sans retenue – une attaque par « déni de service ». C'est pourquoi a été prévu un mécanisme qui interdit cela. Lorsqu'on demande à utiliser un programme déposé sur la blockchain, il faut associer à cette demande une certaine somme, très faible, mais cruciale pour le bon fonctionnement de l'ensemble du système.

Ces sommes dépensées par les utilisateurs d'un programme récompensent des membres du réseau, les nœuds principaux ou « mineurs », qui organisent l'évolution et le contrôle de la blockchain. Les autres utilisateurs se contentent de profiter de l'ordinateur-monde sans participer à son contrôle. Les commissions empêchent les programmes trop gourmands en puissance de tout faire s'effondrer, encouragent les programmes économes en calcul, interdisent les attaques par déni de service et incitent à participer à la surveillance de la blockchain et donc à l'exécution commune de tous les programmes qu'elle porte.

Ajoutons que les mineurs fixent un prix pour les opérations qu'ils exécutent sur la blockchain et si le prix que propose un utilisateur simple de programme est trop faible, les opérations de ce programme attendent. L'utilisateur d'un programme doit proposer une commission raisonnable pour que sa

Bitcoin et Ethereum

Le réseau pair à pair du bitcoin, qui a donné naissance à la monnaie bitcoin, a quelques défauts que le réseau Ethereum, dont est issue la monnaie ether, a tenté de corriger. Voici quelques points de comparaison.

– Le nombre total de bitcoins qui seront émis est 21 millions, et leur émission va en décroissant : aujourd'hui, 12,5 bitcoins sont émis toutes les 10 minutes. Les ethers sont émis à raison de 5 toutes les 12 secondes, et ce rythme restera inchangé. Le nombre d'ethers en circulation continuera donc de croître indéfiniment, mais le nombre d'ethers émis par an sera de plus en plus faible comparé au nombre d'éthers déjà en circulation. La pression d'inflation créée par les nouvelles émissions tendra donc vers zéro, comme pour le bitcoin.

– L'ordinateur-monde du bitcoin ne peut qu'effectuer des transactions entre comptes : sa blockchain est une liste ordonnée de transactions. L'ordinateur-monde d'Ethereum effectue des opérations plus complexes. Sa blockchain contient des transactions et des programmes qui sont exécutés sans que personne ne puisse en prendre le contrôle ou les arrêter. Cela permet donc facilement la création d'organisations autonomes décentralisées (DAO), outil de base de la création de confiance entre entités indépendantes.

– La taille des pages de la blockchain du bitcoin est limitée et exige un accord entre les mineurs pour évoluer, accord introuvable aujourd'hui. La taille des pages de la blockchain Ethereum n'est pas bornée.

– Le nombre de transactions par seconde que peut traiter le réseau bitcoin est d'environ 5. Pour Ethereum, c'est environ trois fois plus.

– Le coût d'une transaction entre comptes bitcoin est en principe gratuit, sauf qu'il faut accepter de payer une commission directement liée à la taille de la transaction pour qu'elle soit validée (cette obligation récente résulte du problème de la taille bornée des pages de la blockchain). Le coût d'une transaction pour l'ether dépend de sa complexité et de l'utilisation qu'elle fait des ressources des machines exécutant les programmes.

- La valeur des bitcoins en circulation est aujourd'hui (en septembre 2016) dix fois supérieure à celle des ethers.

- Les équipes travaillant autour du bitcoin sont sensiblement plus nombreuses que celles travaillant pour l'ether.

– Le procédé d'incitation à participer à la surveillance de la blockchain du bitcoin, appelé « preuve de travail », a conduit au développement de puces spécialisées (ASIC) et à une compétition, jugée absurde, provoquant une dépense électrique considérable et une concentration des mineurs aujourd'hui majoritairement en Chine. Le procédé équivalent pour Ethereum ne permet pas, semble-t-il, le développement de puces spécialisées et évite donc plusieurs des inconvénients du bitcoin.

© Fat Jackey ; Anastasiia Bakal/shutterstock.com

demande soit prise en compte. Un marché s'établit entre les mineurs et les utilisateurs. Le système, subtil, est fondé sur des idées économiques qui y jouent un rôle régulateur. Ces constructions informatiques modernes que sont les ordinateurs à blockchain ont, en leur cœur même, des unités de valeur économique qu'ils manipulent et sans lesquelles ils ne pourraient pas exister. Il faut maîtriser une forme d'« économie numérique fondamentale » pour concevoir les ordinateurs à blockchain et cela implique en particulier que les programmes déposés sur la blockchain constituent eux-mêmes des acteurs économiques.

Limites et dangers divers

Tout ce que nous avons dit est très réjouissant et semble parfait… en théorie. La délicatesse et la fragilité de ces constructions, on s'en doute, créent des risques et des difficultés. Cette informatique du futur est dans une phase expérimentale qui n'exclut pas les accidents, voire les catastrophes.

Citons six points délicats pour lesquels des progrès sont à faire avant d'envisager une utilisation à grande échelle des ordinateurs à blockchain :

– l'accroissement de la taille de la blockchain ne doit pas être sans limite, de même que la quantité de calcul exécutée par les mineurs d'un ordinateur à blockchain. On espère profiter de l'augmentation de la puissance des dispositifs informatiques, qui, selon la loi de Moore, double tous les deux ans. Cependant, cela ne permet pas tout, d'autant que la loi de Moore s'essouffle. Le trop grand succès d'un ordinateur-monde provoquerait un problème d'encombrement, voire le paralyserait ;

– les algorithmes cryptographiques utilisés pour assurer l'intégrité de la blockchain, la signature des transactions et le bon fonctionnement d'un réseau pair à pair ne sont pas sûrs à 100 %. L'exploitation d'une faille dans l'un d'eux pourrait tout démolir, d'où le soin particulier qui doit présider à leur choix et la nécessité de prévoir des procédures efficaces de substitution d'un algorithme par un autre en cas de faiblesse identifiée ;

– les programmes, même s'ils sont publics, ne sont pas nécessairement sans erreurs. Leurs bugs peuvent entraîner de graves dysfonctionnements, voire autoriser un pirate ayant repéré l'un d'eux à s'emparer de l'argent stocké dans le compte d'une DAO.

C'est ce qui s'est produit le 17 juin 2016, quand l'exploitation d'une erreur dans le programme d'une DAO de la blockchain d'Ethereum a permis à un programmeur malin (resté anonyme) de s'emparer temporairement de l'équivalent de 50 millions d'euros. Heureusement, le pirate informatique n'a pas pu les faire sortir de la blockchain et en profiter. Une opération appelée *hard fork* a permis de rendre l'argent déplacé à ceux à qui il appartenait, et tout est rentré dans l'ordre le 9 juillet, à la nuance près que des utilisateurs insatisfaits de la méthode de traitement du problème ont donné naissance à une version concurrente d'Ethereum. La leçon de cette catastrophe évitée de justesse est que les programmes pour les ordinateurs à blockchain doivent être écrits avec un soin extrême, sans doute en utilisant les méthodes mises en œuvre dans l'industrie aéronautique et les systèmes embarqués ;

– la gouvernance d'un système tel qu'Ethereum est délicate. En théorie, il n'y en a pas besoin, et seules certaines évolutions majeures du système sont effectuées à la suite du vote des mineurs qui détiennent collectivement une forme de pouvoir « démocratique » sur le système. Cependant, en cas d'urgence, une réaction rapide est parfois indispensable. Une réflexion approfondie doit être menée pour résoudre ce dilemme entre automaticité du système, utile à la création de la confiance, et réactivité, essentielle dans certaines situations ;

– rien n'empêche une DAO d'avoir été conçue pour exploiter ses utilisateurs au bénéfice de son créateur. Il faut donc pouvoir exercer un certain contrôle sur les DAO créées. Comment l'organiser sans annuler les bénéfices des principes fondateurs des DAO ?

– dernier point : le statut légal et juridique des DAO est à concevoir et définir précisément. Cela ne sera pas simple.

Expérimentale aujourd'hui, cette nouvelle technologie des ordinateurs-mondes nous réserve toutes sortes de surprises ! ■

L'AUTEUR

J.-P. DELAHAYE est professeur émérite à l'université de Lille et chercheur au Centre de recherche en informatique, signal et automatique de Lille (CRISTAL).

BIBLIOGRAPHIE

Le projet Ethereum : https://www.ethereum.org https://www.ethereum-france.com

Understanding Ethereum, *CoinDesk*, 2016 : http://bit.ly/2cTEHMK.

J.-P. Delahaye, **Les blockchains, clefs d'un nouveau monde**, *Pour la Science*, n° 449, pp. 80-85, mars 2015 ; **Bitcoin, la cryptomonnaie**, *Pour la Science*, n° 434, pp. 80-85, décembre 2013.

A. Kosba *et al.*, **Hawk : The blockchain model of cryptography and privacy-preserving smart contracts**, 2015 (https:// eprint.iacr.org/2015/675.pdf).

Retrouvez la rubrique Logique & calcul sur www.pourlascience.fr