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