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