moment de sa création à celui qui en demande l'ouverture. Des programmes appelés *wallets* ou porte-monnaie, fonctionnant sur smartphone ou microordinateur, permettent à chacun de créer ses propres comptes, en général gratuitement et sans avoir à fournir son identité. Cet anonymat de la détention des comptes rend les monnaies cryptographiques analogues à l'argent liquide circulant sous forme de pièces ou de billets : on détient anonymement des unités monétaires, on en reçoit et on en dépense.

Si vous connaissez la clé secrète d'un compte, vous pouvez agir sur lui et par exemple demander un virement d'une unité de ce compte en faveur d'un autre compte dont vous connaissez le numéro. Cette opération est une transaction et tous les nœuds du réseau qui gardent la blockchain en sont informés ; ils modifieront de la même façon leur copie de la blockchain pour prendre en compte la modification des soldes des comptes après le virement. Toutes les copies de la blockchain sont synchronisées et parfaitement identiques.

Le contrôle collectif et consensuel de la blockchain, donc sur les comptes en général, engendre la confiance et permet de croire que détenir une unité de la cryptomonnaie vaut quelque chose. Cette valeur d'une unité s'établit comme pour une action boursière ou une œuvre d'art, par la rencontre entre ceux qui veulent en vendre et ceux qui veulent en acheter et qui se mettent d'accord sur un prix d'échange. Des sites internet appelés *exchanges*, ou « plateformes d'échange », organisent ces rencontres. Certaines cryptomonnaies ne valent presque rien, d'autres comme les bitcoins valent assez cher (le 29 mars 2019, 1 bitcoin valait environ 3650 euros, ou 4100 dollars). Pour comparer l'importance des cryptomonnaies, on multiplie le nombre d'unités dans la blockchain par le cours d'une unité en dollars. Le 29 mars 2019, cette capitalisation globale atteignait environ 72 milliards de dollars pour les bitcoins, 15 pour les ethers et 13 pour les ripples. Douze monnaies cryptographiques dépassaient à cette date une capitalisation de 1 milliard de dollars (voir https://coinmarketcap.com).

FONCTIONNEMENT PARFAIT SANS AUTORITÉ CENTRALE

Avant la mise en marche du réseau des bitcoins le 3 janvier 2009, on pensait impossible de faire fonctionner une monnaie sans autorité centrale. Le protocole du bitcoin a montré que c'est possible. Il fonctionne depuis plus de dix ans et n'a jamais été piraté. Les escroqueries à base de bitcoins, les vols de bitcoins, leur utilisation pour des actions frauduleuses sont comme les escroqueries à base de dollars, les vols de dollars, et >

1 UNE INDUSTRIE AUTOUR DES CRYPTOMONNAIES

Composants électroniques dans une ferme de minage de bitcoins.

Divers types d'activités s'organisent autour des cryptomonnaies et donnent naissance à des entreprises, parfois importantes, reposant sur des modèles économiques variés. Mentionnons-en une liste en notant que, souvent, plusieurs types d'activités sont mêlés au sein d'une même société.

- Des sociétés vendent des prestations de formation ou de développement d'applications liées aux cryptomonnaies et aux blockchains.
- Des sociétés collectent des informations autour des cryptomonnaies, les publient, les vendent, etc.
- Les plateformes d'échange jouent le rôle de bureau de change. Elles permettent par exemple d'acheter des ethers en échange d'euros. Elles offrent souvent la possibilité de garder vos achats, ce qui vous évite d'avoir à gérer les clés de vos comptes. Elles gagnent de l'argent en faisant payer des commissions pour les opérations qu'elles réalisent. En France et dans de nombreux pays, elles doivent connaître leurs utilisateurs qui, pour s'inscrire, indiquent et prouvent leur identité.
- Des développeurs et fabricants vendent des porte-monnaie électroniques, logiciels ou matériels, permettant de détenir en propre des cryptomonnaies, c'est-à-dire de gérer soi-même les clés de ses comptes. La société française Ledger propose par exemple des dispositifs matériels de sécurisation des clés et des comptes de cryptomonnaies ; elle est la première de sa catégorie et a vendu plus d'un million de ses dispositifs de sécurisation.
- Les concepteurs et fabricants d'outils de minage. Des matériels spécialisés sont souvent nécessaires pour participer aux concours de calcul que sont les preuves de travail. Ce sont soit des assemblages de circuits ASIC *(Application Specific Integrated Circuit)*, soit, par exemple pour ethereum, des cartes graphiques. En 2017 et 2018, le marché de ces matériels a représenté plusieurs milliards de dollars. Des firmes sont nées de ce commerce (le chinois Bitmain par exemple) ou en ont profité (fabricants de cartes graphiques).
- Des sociétés achètent du matériel de minage et de l'électricité et montent des « fermes de minage » qu'elles font fonctionner. Elles gagnent des unités de cryptomonnaies. Leur rentabilité dépend de la concurrence, du prix qu'elles paient l'électricité et du cours des cryptomonnaies. Plusieurs milliards de dollars sont à gagner chaque année. Cela a provoqué l'apparition d'importantes firmes. Elles se trouvent en Chine, en Islande, au Canada et là où on peut acheter de l'électricité à moindre coût. Suite à la baisse des cours des cryptomonnaies en 2018, elles sont nombreuses aujourd'hui à rencontrer des difficultés et parfois doivent cesser leur activité. La firme française Bigblock a construit un modèle original : elle déplace, installe et fait fonctionner pour qui le veut des outils de minage dans son usine au Kazakhstan, où elle réussit à acheter de l'électricité à un prix très bas (0,026 euro le kWh).

> l'utilisation des dollars pour mener des actions illicites : elles ne concernent pas la monnaie en elle-même, son émission ni son mode de circulation. Ce miracle d'une monnaie numérique sans autorité centrale résulte de l'utilisation de la cryptologie (pour organiser la blockchain et permettre le système de signatures qui protègent les transactions), de la fiabilité des réseaux informatiques et de la capacité de calcul et de mémorisation des ordinateurs modernes.

Le fonctionnement du réseau repose sur les nœuds validateurs qui sont des ordinateurs volontaires toujours connectés, surveillant les transactions et conservant chacun une copie de la blockchain en la mettant à jour en fonction des transactions qui circulent. Il n'est heureusement pas nécessaire d'être un tel nœud validateur pour disposer d'un compte et utiliser la cryptomonnaie : la plupart des détenteurs de comptes ne sont pas des nœuds validateurs.

DES INCITATIONS

Pour le travail effectué, une récompense est attribuée aux nœuds validateurs : cette incitation rétribue le service fourni et permet à la cryptomonnaie d'exister. La distribution de cette récompense se fait parfois (et en particulier dans le cas des bitcoins et des ethers) par l'attribution aux nœuds validateurs de nouvelles unités de la cryptomonnaie. Dans le cas des bitcoins, de nouvelles unités sont créées toutes les dix minutes et sont attribuées à un ordinateur du réseau à la suite d'un concours entre les nœuds validateurs. Le concours récompense le premier nœud validateur ayant réussi à résoudre un problème de nature mathématique qui nécessite beaucoup de calculs. Ce mode de distribution de l'incitation est appelé preuve de travail ; il a conduit au développement d'une industrie nommée minage, car on extrait de nouveaux bitcoins comme on extrait de l'or d'une mine, mais en menant des calculs massifs plutôt qu'en creusant le sol. Malheureusement, la concurrence fait que ce concours répété est devenu énergivore. Nous y reviendrons quand nous évoquerons d'autres moyens de distribuer l'incitation.

Venons-en aux variantes et perfectionnements possibles.

L'anonymat des comptes est, selon les avis, trop faible ou trop fort. Il est trop fort pour certains qui y voient un danger. En effet, une monnaie cryptographique comme le bitcoin permet de détenir et d'utiliser un compte sans jamais révéler son identité, ce qui permet de manipuler les unités de la cryptomonnaie comme de l'argent liquide – mais en fait bien plus liquide que des billets ou des pièces, puisque vous pouvez envoyer en quelques minutes et en toute discrétion l'équivalent de millions de dollars ou d'euros d'un pays vers n'importe quel autre. Cet anonymat est prisé pour le blanchiment d'argent, le paiement de rançons et toutes sortes de trafics. Il en résulte une méfiance envers les cryptomonnaies. Des cryptomonnaies d'État sont annoncées sans qu'on sache toujours leurs propriétés et en particulier leur attitude vis-à-vis de l'anonymat. Elles pourraient exiger des utilisateurs qu'ils n'ouvrent de comptes qu'après avoir donné et prouvé leur identité.

Le ripple, la cryptomonnaie la mieux acceptée du monde bancaire, a introduit des procédures dites de KYC (*know your consumer*) pour limiter l'anonymat. La cryptomonnaie electroneum (88e en mars 2019) est une cryptomonnaie qui exige de connaître l'identité des détenteurs de ses comptes. Notons aussi que les plateformes d'échange, qui nous sont indispensables pour acheter ou vendre des monnaies cryptographiques contre les monnaies fiduciaires habituelles, exigent presque toujours l'identité de leurs utilisateurs. En résumé, détenir et faire circuler anonymement des monnaies cryptographiques est facile, mais en échanger contre des dollars ou des euros ne l'est pas !

L'ANONYMAT POSE QUESTION

De ce fait, l'anonymat d'une cryptomonnaie de base (comme le bitcoin ou l'ether) est jugé imparfait par certains utilisateurs. Toutes les transactions sont inscrites en clair sur la blockchain auquel tout le monde a accès ; cela permet de suivre, de numéro de compte en numéro de compte, le déplacement des sommes importantes. Dans certains cas, cela a permis d'identifier le détenteur d'un compte… et de l'arrêter car il était établi que des trafics illicites étaient liés aux sommes qui circulaient.

Cette situation fait que certains esprits attachés à l'anonymat ont imaginé des modifications dans la conception des blockchains pour empêcher le suivi du déplacement des sommes de compte en compte. Parmi les cryptomonnaies ayant accru cet anonymat en rendant (presque) impossible le suivi des transactions, mentionnons monero, dash, zcash, verge, komodo, PIVX, hirozen, zcoin, nav coin. Le bitcoin intéresse aujourd'hui beaucoup moins les malfrats, qui se sont reportés sur ces monnaies à l'anonymat renforcé et particulièrement sur monero. Plusieurs pays, dont la Chine et la Corée du Sud, ont entrepris d'interdire tout échange anonyme impliquant des cryptomonnaies.

SMART CONTRACTS, ICO ET APPLICATIONS DÉCENTRALISÉES

Lorsqu'une transaction (un virement d'un compte A vers un compte B) est signée et lancée par le détenteur d'un compte à partir de