AU-DELÀ DU BITCOIN

L'idée des cryptomonnaies, concrétisée pour la première fois avec le bitcoin, a donné naissance à une industrie foisonnante et variée, qui propose nombre d'améliorations.

L'AUTEUR

JEAN-PAUL DELAHAYE
professeur émérite à l'université de Lille et chercheur au Centre de recherche en informatique, signal et automatique de Lille (Cristal)

Jean-Paul Delahaye a récemment publié : **Les Mathématiciens se plient au jeu**, une sélection de ses chroniques parues dans *Pour la Science* (Belin, 2017).

Il est rare qu'une invention technique soit parfaite à sa naissance. Nos automobiles et nos avions ressemblent assez peu aux premiers exemplaires. C'est vrai aussi des machines à laver, des téléviseurs, des téléphones et surtout des ordinateurs. Le domaine des monnaies cryptographiques, ou cryptomonnaies, bénéficie aussi de cette diversification et de ce perfectionnement progressif. Le bitcoin fut la première de ces monnaies numériques et si, bizarrement, certains le considèrent comme indépassable, le foisonnement de variantes montre qu'il n'est que le premier pas d'un processus évolutif technique.

CE QU'EST UNE CRYPTOMONNAIE

Nous décrirons un modèle simplifié des cryptomonnaies, parfois prudemment dénommées cryptoactifs, et nous verrons comment en dérivent les variantes qui s'écartent du modèle de base.

La première caractéristique d'une cryptomonnaie est d'être numérique : jamais vous ne tiendrez en main un bitcoin, un ripple ou un ether (du réseau Ethereum), qui sont les trois plus importantes cryptomonnaies, dans une famille qui en compte plus de deux mille.

L'existence d'une telle monnaie se fonde sur celle de comptes informatiques et d'une base de données, appelée *blockchain*, ou « chaîne de pages », détenant toutes les informations sur l'état de tous les comptes. Cette base de données des comptes est recopiée dans la mémoire d'une multitude d'ordinateurs, les nœuds validateurs (ou nœuds complets), organisés en réseau et communiquant par Internet. La base de données permet à chaque nœud validateur de connaître l'état de tous les comptes : le compte A détient n unités de la monnaie, le compte B en détient m, etc. Tout le monde peut connaître l'état de tous les comptes en interrogeant certains nœuds validateurs.

Cette recopie de la blockchain dans la mémoire de chaque nœud validateur la rend infalsifiable : si un détenteur de la blockchain veut la modifier en sa faveur, par exemple pour s'attribuer plus d'unités monétaires, les autres refuseront sa version falsifiée et s'en tiendront à la version commune. La monnaie est décentralisée et sans autorité centrale : personne n'a seul le pouvoir d'en perturber le fonctionnement, qui s'appuie sur un consensus.

UN PROTOCOLE, DES COMPTES, DES TRANSACTIONS

Le protocole de fonctionnement d'une cryptomonnaie est déterminé avant son émission et en indique les propriétés particulières, par exemple en fixant la fréquence d'ajout de nouvelles pages à la blockchain. Le protocole organise le rythme des émissions de nouvelles unités monétaires et leur circulation d'un compte à un autre. Ce protocole est initialement choisi par un ou plusieurs spécialistes, mais une fois programmé et lancé, plus personne en particulier ne le contrôle et il ne peut être modifié qu'après un accord général, selon les règles d'un protocole.

Détenir un compte, c'est connaître la clé secrète du compte, qui est délivrée au

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 >

UNE INDUSTRIE AUTOUR DES CRYPTOMONNAIES

1

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).