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)

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

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

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

son ordinateur ou de son smartphone, elle circule sur le réseau des nœuds validateurs qui ne peuvent que l'accepter et exécuter ce qu'elle demande. L'opération est irréversible. Cette irréversibilité n'existe pas pour les virements dans le monde bancaire classique, où les établissements gardent pendant plusieurs jours la possibilité d'annuler un virement. Cette irréversibilité des transactions en cryptomonnaies est intéressante et a été généralisée avec ce qu'on dénomme des contrats intelligents, ou *smart contracts*. Ce sont des programmes qu'on dépose sur la blockchain de certaines cryptomonnaies et qui ont la capacité de détenir des unités monétaires, d'en recevoir et d'en envoyer automatiquement.

La première cryptomonnaie à offrir un langage puissant pour écrire ces *smart contracts* était ethereum (*voir « Du bitcoin à ethereum : l'ordinateur-monde »*, Pour la Science *de novembre 2016, pp. 104-109*). L'irréversibilité devient pour un *smart contract* l'impossibilité d'en arrêter le fonctionnement, qui est simultané sur chaque nœud validateur. Cela interdit de faire exécuter au programme autre chose que ce qui est prévu. Ces programmes qui, une fois définis, ne peuvent plus être arrêtés ou modifiés parce que leur fonctionnement provient du consensus d'exécution du réseau, constituent une nouveauté informatique extraordinaire. Cet ordinateur mondial, décentralisé, parfaitement fiable fait ce qu'on lui demande de faire sans que personne ne puisse l'interrompre ou le corrompre.

Cela permet par exemple de programmer des jeux d'argent et de pari où l'organisateur ne peut pas refuser de payer et ne peut partir avec la caisse quand il perd trop. Le terme d'applications décentralisées (DApp, en abrégé anglo-saxon) est souvent utilisé pour désigner ces *smart contracts*.

Grâce à ces *smart contracts*, on crée des cryptomonnaies qui ont les mêmes propriétés que celles reposant sur des blockchains spécifiques : elles sont sans autorité centrale et surveillées, indirectement maintenant, par les nœuds validateurs d'un réseau. En clair, grâce aux cryptomonnaies permettant les *smart contracts*, on définit facilement de nouvelles monnaies décentralisées sans avoir à mettre en place un réseau nouveau de nœuds validateurs.

Cette possibilité de disposer de l'équivalent d'une blockchain particulière à moindre coût en s'appuyant par exemple sur la blockchain ethereum a engendré l'apparition rapide de nouvelles cryptomonnaies, dont le nombre a explosé depuis 2016. Des cryptomonnaies liées à certaines entreprises voulant lever des fonds ont été introduites par dizaines. Les unités monétaires de ces cryptomonnaies se nomment des jetons (*tokens*) et ces opérations de >

2

LES ICO OU PRÉÉMISSIONS DE JETONS

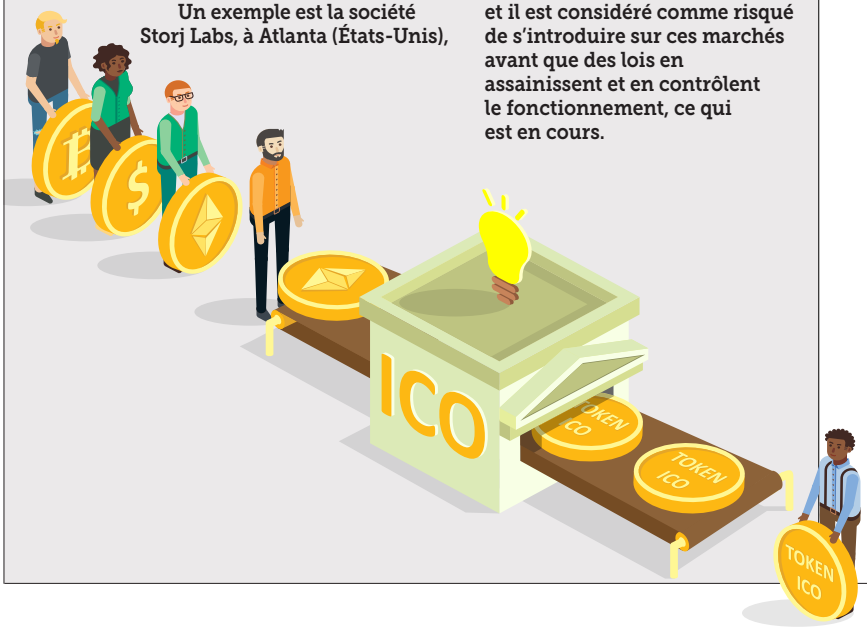
Une ICO (pour *initial coin offering*, ou « préémission de jetons ») est une méthode de levée de fonds fondée sur une cryptomonnaie liée à l'entreprise qui veut se financer. Les jetons de la cryptomonnaie sont en général créés à l'aide d'un *smart contract (voir le texte principal)*. On peut acheter des jetons pendant la phase de démarrage de l'entreprise. Ces jetons sont cotés et échangeables sur les plateformes d'échange de cryptomonnaies. Le plus souvent le bitcoin ou l'ether sert de monnaie intermédiaire : on achète des bitcoins pour ensuite les échanger contre des jetons de l'ICO.

Les jetons de l'ICO donnent des droits particuliers concernant l'entreprise qui les a émis : droits de vote, droits d'usage des services à prix intéressants, etc. Contrairement aux actions mises en circulation lors d'une IPO (*initial public offering*, en français « introduction en Bourse »), les jetons ne représentent pas des parts de l'entreprise. Acheter les jetons d'une ICO revient à prépayer les services qui vont être proposés.

Un exemple est la société Storj Labs, à Atlanta (États-Unis), qui crée un service de stockage massif décentralisé. Les fichiers informatiques à stocker sont chiffrés et découpés en morceaux. On les copie alors – avec des redondances pour se protéger des accidents – dans la mémoire des ordinateurs acceptant de participer au réseau de stockage. La capacité du réseau dépasse 100 pétaoctets (soit 10^{17} octets), et l'objectif est d'arriver à plusieurs exaoctets (10^{18} octets). Le réseau est déjà composé de 150 000 ordinateurs capables de détenir des morceaux de fichiers confiés à Storj répartis dans 200 pays.

La société Storj Labs a levé début 2017 l'équivalent de 30 millions de dollars *via* une ICO. Leur jeton, le storjcoin, permet d'acheter de l'espace de stockage sur le réseau Storj ; il représente donc un accès privilégié aux services développés. La capitalisation des jetons Storj en février 2019, (victime de la baise générale des cours de l'année 2018) s'élevait à 18 millions de dollars. Si la société réussit, ses jetons se valoriseront.

Contrairement aux IPO, les ICO sont mal réglementées et il est considéré comme risqué de s'introduire sur ces marchés avant que des lois en assainissent et en contrôlent le fonctionnement, ce qui est en cours.



3 MONTÉE EN FLÈCHE DES STABLECOINS

Puisque la volatilité des cours des monnaies cryptographiques rend impossible leur usage comme « réserve de valeur », ou même comme instrument de paiement, il fallait empêcher cette volatilité.

L'idée la plus simple est d'offrir à tout détenteur d'une unité de la cryptomonnaie la capacité de l'échanger contre un actif précis ayant une valeur qui, par définition, sera considérée comme fixe, par exemple un dollar. La possibilité de cet échange rend absurde d'attribuer à l'unité en question une valeur moindre. Si, en plus, à chaque fois que quelqu'un veut disposer d'une unité de cette cryptomonnaie, on lui donne la possibilité de l'acquérir à ce coût fixé à l'avance, le cours de la cryptomonnaie ne pourra pas monter. C'est l'idée des *stablecoins*, ou « jetons stables ». Ces *stablecoins*, comme les cryptomonnaies, reposent directement ou indirectement sur une blockchain, ce qui assure la nature décentralisée et irréversible des transactions et du fonctionnement des comptes, et permet l'anonymat. Cependant, il faut que celui qui propose ces échanges 1 contre 1 (par exemple avec le dollar) soit crédible. Il faut pour cela qu'il organise un système d'audit indépendant attestant qu'il met en réserve la contrepartie des unités qu'il fait circuler. Cette contrepartie gardée en réserve par un acteur déterminé constitue un aspect centralisé de la cryptomonnaie. Ceux qui sont attachés à l'idée d'une décentralisation complète considèrent cela regrettable. Insistons sur le fait que la gestion des comptes est décentralisée et qu'un tel *stablecoin* n'est donc pas centralisé comme l'est une monnaie d'État : on gagne donc bien quelque chose, en plus de la fluidité et de la stabilité du cours, avec les *stablecoins*.

Les principales *stablecoins*, avec leur capitalisation et leur cours en dollars ($), sont :
USD Tether : 2 032 525 000 $
1 USDT = 1,00 $
USD coin : 247 268 000 $
1 USDC = 1,00 $
True USD : 200 244 000 $
1 TUSD = 1,01 $
Nano : 135 067 000 $
1 Nano = 1,01 $
Paxos Standard : 118 657 000 $
1 PAX = 1,00 $
Dai : 87 789 000 $
1 DAI = 0,99 $

Le *stablecoin* dai fonctionne selon un mécanisme différent de celui décrit plus haut. Ce mécanisme est, lui, totalement décentralisé et s'appuie sur une surcontrepartie en cryptomonnaie (par exemple de 1,5 dollar de cryptomonnaie pour 1 dollar de *stablecoin*) qui permet de garantir la stabilité… à la condition que les variations de cours de la cryptomonnaie utilisée pour adosser le *stablecoin* ne soient pas trop brusques. De nouveaux modèles de *stablecoins* totalement décentralisés sont en cours d'expérimentation.

Le succès des *stablecoins* en 2018 a été remarquable. De 30 projets de *stablecoins* (dont 9 en fonctionnement) au début de 2018, on est passé début 2019 à plus de 160 projets (dont 28 fonctionnent). La capitalisation boursière totale de ces *stablecoins* a doublé durant la même période, passant d'environ 1,5 milliard à presque 3 milliards de dollars. Notons aussi que les *stablecoins* pourraient être plus facilement acceptées par les autorités monétaires : par exemple, les régulateurs financiers de l'État du Texas, aux États-Unis, envisagent de donner aux *stablecoins* un statut de monnaie au même titre que l'euro ou le yen.

> levée de fonds se nomment ICO, pour *initial coin offering*, par analogie avec IPO, pour *initial public offering* («introduction en Bourse»).

Plusieurs milliards de dollars ont pu ainsi être trouvés pour le financement de start-up, qui travaillent en général dans le domaine des cryptomonnaies ou des blockchains. Cependant, contrairement aux IPO, qui sont très réglementées, les ICO ne le sont pas assez et elles ont été utilisées pour organiser diverses escroqueries. Elles sont interdites en Chine et les autorités financières de nombreux pays invitent à s'en méfier. L'émission et la manipulation de ces jetons sont fiables, mais pas ce qu'ils représentent, car les entreprises financées par l'achat de ces jetons sont parfois des coquilles vides. En France, l'Autorité des marchés financiers (AMF) va attribuer des labels pour que les acheteurs intéressés par les ICO puissent y voir clair.

Précisons que d'autres cryptomonnaies ont suivi ethereum en offrant la possibilité sur leur blockchain de déposer des *smart contracts*. Le réseau des bitcoins ne permet pas l'écriture de *smart contracts* qui seraient déposés sur sa blockchain, mais une blockchain connectée à celle des bitcoins dénommée *rootstock* le permet. Les cryptomonnaies ripple, EOS, NEO, cardano autorisent aussi la création de *smart contracts*.

DES CRYPTOMONNAIES SANS PREUVE DE TRAVAIL

Les monnaies fonctionnant avec des «preuves de travail» pour récompenser ceux qui acceptent d'être des nœuds validateurs du réseau et contribuent à ce qu'il fonctionne ont deux graves défauts. Le premier est que leur fonctionnement et leur sécurité exigent une dépense continue et importante d'électricité. L'article publié en février 2018 dans cette rubrique «La folie électrique du bitcoin» (pp. 80-85) détaillait ce problème. Une mise à jour des chiffres de cet article donne comme conclusion qu'aujourd'hui la dépense annuelle électrique du réseau des bitcoins est supérieure à 40 térawattheures (TWh) d'électricité. C'est équivalent à ce que produisent en un an cinq réacteurs nucléaires! Par comparaison, les *datacenters* de Google dépensent moins de 6 TWh par an.

Le second grave défaut des cryptomonnaies utilisant des preuves de travail est que cela crée pour elles un handicap concurrentiel face aux monnaies cryptographiques n'utilisant pas les preuves de travail.

En effet, le fonctionnement d'un réseau de cryptomonnaies a un certain coût, qui d'une façon ou d'une autre doit être payé par les utilisateurs. Les émissions nouvelles d'unités monétaires créent une pression d'inflation et font perdre de la valeur aux unités déjà émises (ce qui est une façon indirecte de faire payer

les utilisateurs). Même si les fortes variations de cours aujourd'hui masquent ce coût, il faudra le prendre en compte à moyen terme. Les commissions directement versées aux nœuds validateurs du réseau, ou d'autres systèmes encore, organisent ce paiement des utilisateurs vers les nœuds validateurs. Dans le cas des monnaies cryptographiques utilisant la preuve de travail, le coût des matériels de minage et de l'électricité sera ainsi payé par les utilisateurs. Ces sommes payées ne sont pas des bénéfices nets pour les nœuds validateurs, car ils doivent payer leur matériel et leur électricité. Aujourd'hui, après la baisse des cours du bitcoin, les nœuds validateurs perdent souvent en amortissement de leur matériel et en électricité plus de 90% de ce qu'ils gagnent: une cryptomonnaie à base de preuve de travail coûtera à terme beaucoup plus aux utilisateurs qu'une monnaie qui s'en passera.

Les autres systèmes les plus utilisés pour remplacer les preuves de travail sont les «preuves d'enjeu». Dans le système des preuves d'enjeu, les nœuds validateurs du réseau (parfois appelés *masternodes*) sont rémunérés en proportion des sommes qu'ils déposent et qui sont séquestrées par le réseau. Ce dépôt temporaire d'argent remplace l'investissement en matériel et la dépense en électricité des preuves de travail. Finalement, il ne coûte rien aux nœuds validateurs qui peuvent récupérer les sommes séquestrées (le protocole prévoit qu'à sa demande, celui qui a déposé l'agent puisse le retirer). Un nœud validateur sur une blockchain fonctionnant par preuve d'enjeu est moins coûteux qu'avec le système des preuves de travail.

Les cryptomonnaies fonctionnant avec ces preuves d'enjeu détiennent aujourd'hui plusieurs milliards de dollars et résistent aussi bien aux attaques que les cryptomonnaies fonctionnant par les preuves de travail. Un autre avantage de ces preuves d'enjeu est que le nombre de nœuds validateurs peut être limité, ce qui accélère le fonctionnement des échanges et conduit à une plus grande capacité en nombre de transactions par seconde.

D'autres systèmes n'entraînant pas la consommation démente des preuves de travail sont aussi utilisés, dont celui des «jetons brûlés»: pour utiliser les services de la blockchain, vous devez acheter des jetons et ils sont détruits quand vous utilisez ses services, ce qui est comparable au système des timbres-poste… utilisés depuis des siècles dans le monde entier.

L'un des plus graves défauts des cryptomonnaies est leur volatilité. Le cours du bitcoin est par exemple passé de 1000 dollars environ début 2017 à 20000 dollars en décembre 2017, avant de redescendre vers 4000 dollars actuellement. Il se peut que cela soit lié à la relative jeunesse de ces monnaies, mais de nombreux experts considèrent que la volatilité est inévitable du fait de l'absence de régulation par une autorité émettrice. L'existence d'une contrepartie directe, quand par exemple une monnaie est adossée à l'or, ou indirecte quand elle est liée à un État qui s'en porte garant, est aussi évoquée comme facteur de stabilité des cours, dont les cryptomonnaies sont dépourvues.

DES CRYPTOMONNAIES PEU VOLATILES: LES *STABLECOINS*

D'où l'idée de créer et d'adosser une cryptomonnaie à une réserve de valeurs. Cela a été fait, donnant naissance à ce qu'on nomme des *stablecoins* («jetons stables»). La plus importante est tether, émise par la société Tether Unlimited qui assure que pour chaque unité tether émise, elle garde en réserve 1 dollar. Même si la réalité de cette contrepartie a parfois été mise en doute, elle semble suffisamment sérieuse pour que plus de 2 milliards de dollars circulent aujourd'hui sous forme de tethers. Une autre preuve de la confiance qui s'est établie à propos de cette cryptomonnaie stable est que le cours du tether est de 1,00 dollar (29 mars 2019) et que depuis plus d'un an, il est toujours resté entre 0,96 dollar et 1,03 dollar. L'année 2018 a été celle de ce nouveau type de cryptomonnaies qui se développera en 2019. Des systèmes d'audit scrupuleux assurent que les contreparties annoncées sont réelles.

Le fait qu'une firme soit liée et garante de l'émission d'une telle cryptomonnaie s'oppose à l'idéal de décentralisation totale qui était l'une des motivations des créateurs du bitcoin. Cependant, l'échec relatif des monnaies cryptographiques classiques, dû notamment à la volatilité extrême de leur cours, et la solidité des procédures de contrôle de la contrepartie qu'offrent les *stablecoins* suggèrent qu'elles vont prochainement jouer un rôle important dans cette période nouvelle de l'histoire des monnaies, commencée il y a dix ans avec les bitcoins.

Notons aussi qu'à part l'adossement à une réserve de valeur, un *stablecoin* tel que le tether est décentralisé pour le suivi des transactions et que des modèles de *stablecoins* totalement décentralisés sont expérimentés, qui, s'ils se révèlent satisfaisants, répondront aux attentes de ceux qui accordent de l'importance à la décentralisation totale.

La combinaison des *smart contracts* et des *stablecoins* est sur le point de créer le véritable départ d'un monde de monnaies numériques programmables pouvant circuler rapidement de manière sûre, irréversible, sans presque aucun coût de fonctionnement, sans dépense énergétique exagérée, éventuellement anonyme et dont les cours ne sont plus sujets aux folles variations du bitcoin et de ses émules. ■

BIBLIOGRAPHIE

J. Favier *et al.*, **Bitcoin - Métamorphoses. De l'or des fous à l'or numérique ?** Dunod, 2018.

OPECST (Office parlementaire d'évaluation des choix scientifiques et technologiques), **Les enjeux technologiques des blockchains**, 2018 : http://www.senat.fr/rap/r17-584/r17-5841.pdf

J.-P. Landau et A. Genais, **Les crypto-monnaies,** rapport au ministre de l'Économie et des Finances, 4 juillet 2018 : https://bit.ly/2UXAZqn

Article **Stablecoin** sur Wikipedia (consulté en février 2019) : https://en.wikipedia.org/wiki/Stablecoin

J.-P. Delahaye, **Consommation électrique des crypto-monnaies et des blockchains**, document pour la réunion de travail de France-Stratégie sur « La consommation électrique des technologies disruptives » le 4 juin 2018 : https://bit.ly/2FvENsE