> 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