1. La signature et l'identification d'un document

Un protocole de signature à double clef est la donnée de deux fonctions f et g permettant de signer les messages et d'interpréter les signatures. Ces fonctions sont connues de tous. Nous ne nous préoccupons pas ici de la teneur du message, mais seulement de son identification.

À Alice sont associées deux clefs, A_{pri} (clef privée) et A_{pub} (clef publique). Ce sont des suites de chiffres. A_{pub} est accessible à tous, mais la clef A_{pri} n'est connue que d'Alice. Il est impossible en pratique de déduire A_{pri} de la connaissance de A_{pub}.

Les deux fonctions f et g servent à signer un message et à lire la signature.

Soit M un message à signer. Alice applique f aux données A_{pri} et M : $f(A_{pri}, M) = M'$. Ce sera le message signé par Alice. Toute personne ayant en main M' et connaissant la clef publique d'Alice vérifiera que c'est bien Alice qui a signé le message : pour cela, elle appliquera la fonction de lecture g aux données A_{pub} et M', ce qui donne M, car $g(A_{pub}, M') = M$. Le fait qu'il soit nécessaire d'appliquer la clef publique d'Alice à M' pour prendre connaissance du message empêche toute falsification du message M signé.

Il est parfois commode pour Alice de transmettre à la fois M et M', M' servant seulement à contrôler pour ceux qui le veulent qu'Alice a bien signé M avec sa clef privée.

Il existe de nombreuses façons de construire les fonctions f et g, mais la monnaie *bitcoin* est fondée sur la cryptographie à courbes elliptiques. La courbe employée est celle notée secp256k1. On aurait pu utiliser l'algorithme RSA, plus connu, mais il nécessite des clefs plus longues. La sécurité du système *Bitcoin* repose sur l'inviolabilité de la signature.

Les signatures de Napoléon Bonaparte.

collectif de la monnaie (nous verrons plus loin comment).

La gestion d'un porte-monnaie doit être très soigneuse. Si vous le perdez en l'effaçant par mégarde ou si vous oubliez le code secret qui permet d'y accéder, alors son contenu est perdu, comme quand vous lancez par-dessus bord un porte-monnaie réel au milieu de l'océan. De nombreux *bitcoins* ont ainsi été perdus par des utilisateurs imprudents ou négligents. Il n'est pas impossible non plus qu'on vous vole votre porte-monnaie virtuel, par exemple à l'occasion d'une intrusion dans votre ordinateur par un hacker. Pour éviter cela, certains porte-monnaie contenant d'importantes sommes en *bitcoins* sont gardés sur des ordinateurs non connectés au réseau ou éteints.

La cohérence des comptes, et donc la solidité de la monnaie *bitcoin*, se fonde sur un principe général de la théorie *Money is memory* de l'économiste américain Narayana Kocherlakota. Ce principe s'exprime ici sous la forme suivante :

– toutes les transactions faites depuis le début des *bitcoins,* le 3 janvier 2009, sont publiques et, à chaque instant, la somme totale des *bitcoins* émis est connue de tous, ainsi que le contenu de chaque porte-monnaie (mais pas le détenteur de ce porte-monnaie) ;

– seul celui qui connaît la clef secrète d'un porte-monnaie peut dépenser son contenu en envoyant tout ou partie de ce dernier à un autre porte-monnaie, cela à la vue de tous, ce qui permet à tous de connaître à chaque instant le contenu de chaque porte-monnaie ;

– tous ceux qui le souhaitent peuvent participer au calcul général de la répartition des *bitcoins* entre les porte-monnaie, cela à l'aide de logiciels (libres et gratuits) dont la correction est contrôlable par tous.

On n'utilise pas ici la cryptographie à clef publique pour cacher de l'information, mais pour signer les transactions. Toute transaction est irréversible, sauf accord explicite des deux contractants pour réaliser une transaction inverse. Quand vous avez dépensé l'argent d'un porte-monnaie, personne n'a autorité pour demander à celui qui a reçu l'argent de le rendre. C'est là une grande différence avec les monnaies numériques à autorité de contrôle centralisée où, assez fréquemment, des transactions sont annulées, parfois plusieurs jours après leur réalisation, ce qui donne lieu à toutes sortes d'escroqueries. L'absence d'autorité centrale et l'anonymat des comptes font qu'il sera très difficile d'agir sur celui qui détient le porte-monnaie ayant reçu vos *bitcoins*... même s'il ne vous livre pas l'achat que vous pensiez régler.

Ce système simplifié des *bitcoins* a une faille qui a contraint son inventeur à ajouter une série de dispositifs cryptographiques au mécanisme de base. La faille est que le propriétaire d'un porte-monnaie pourrait tenter de dépenser deux fois l'argent qu'il contient. Ces doubles dépenses seraient impossibles si les échanges étaient instantanés sur le réseau et si tout propriétaire d'un porte-monnaie participait au calcul continu du contenu de tous les porte-monnaie : sous cette hypothèse de connectivité totale et parfaite, celui qui recevrait l'argent d'un porte-monnaie déjà vidé (ou insuffisamment pourvu) refuserait la transaction, qui serait simultanément considérée invalide par tous.

Des améliorations

Malheureusement, les échanges électroniques ne sont pas instantanés, et certaines parties d'un réseau sont parfois temporairement déconnectées du reste. De plus, tous les utilisateurs de *bitcoins* ne souhaitent pas participer à la vérification continue de toutes les transactions et au recalcul permanent du solde de la totalité des comptes, car cela demande une grande puissance informatique et beaucoup de mémoire. Il faut donc améliorer le modèle.

Les améliorations se fondent sur une série de protocoles qui rendent la monnaie *bitcoin* résistante aux pannes du réseau ou de certaines machines et aux tentatives de manipulation de la monnaie ou de tricheries (dont les doubles dépenses). Ces perfectionnements rendent aussi facultative la participation au contrôle global des porte-monnaie ; pour éviter que trop peu de nœuds du réseau participent

au contrôle, un système de rémunération est prévu. Ce délicat agencement a étonné les spécialistes et prouve que l'inventeur des *bitcoins* est un cryptologue averti ou un groupe incluant d'excellents cryptologues.

Cette monnaie ne tient que par la cohérence et l'accord unanime de ceux qui y participent et s'entendent sur le contenu de chaque compte, que rien ne matérialise et qu'aucune autorité ne garantit. La construction logicielle et cryptographique doit donc assurer par elle-même que personne ne puisse augmenter le total des *bitcoins* détenus, ni modifier des comptes, sans que tout le monde s'en aperçoive rapidement. Il n'y a pas de police ; la conception même de la monnaie doit donc empêcher la fraude et les dysfonctionnements. Celle de Satoshi Nakamoto y parvient.

Le scepticisme sur la robustesse de la nouvelle monnaie s'atténue. La meilleure preuve est que la monnaie a tenu quatre ans, malgré toutes les attaques qu'elle a subies. C'est pourquoi la valeur actuelle d'un *bitcoin* dépasse 100 euros (mais le *bitcoin* fluctue beaucoup… il vaudra peut-être moins quand vous lirez l'article !).

Une page toutes les dix minutes

L'amélioration du modèle simplifié consiste à créer un cahier de comptes (dont le nom technique est *Blockchain*) qui est complété progressivement par ajout de nouvelles pages de transaction (nommées *blocs*) toutes les dix minutes environ, chaque ajout d'une page étant validé par ceux qui participent à la gestion et à la surveillance décentralisée des comptes. Pour récompenser cette vérification, un tirage au sort désigne toutes les dix minutes environ celui des participants qui ajoute la nouvelle page au cahier de comptes, et qui est rémunéré pour cela par 25 *bitcoins* créés *ex nihilo*. Lorsque la nouvelle page est ajoutée au cahier de comptes, les transactions qui y apparaissent sont validées. Cette création de *bitcoins* est la seule possible, et tous les *bitcoins* existants sont apparus de cette façon.

Lors d'une transaction en ma faveur, mon ordinateur connecté au réseau consulte le cahier de comptes et vérifie que le porte-monnaie qui m'envoie des *bitcoins* ne les a pas déjà dépensés. Cependant, à cause de la possibilité d'une double dépense simultanée, une transaction n'est considérée comme valide que si elle apparaît dans le cahier de comptes. Par conséquent, pour être assuré de l'irréversibilité (par exemple avant d'envoyer le livre qu'on vient de vous acheter en vous faisant parvenir

2. Le protocole d'une transaction

Lorsqu'Alice veut faire un paiement en *bitcoins* à Bernard (par exemple en échange d'un livre), leurs ordinateurs vont opérer une série d'échanges. Ces échanges sont gérés automatiquement par les logiciels installés sur leurs ordinateurs. Les communications sur le réseau *Bitcoin* se font directement entre les deux correspondants, qui y ont des rôles équivalents. On parle de réseaux pair-à-pair (ou P2P, *peer-to-peer*). L'existence de tels réseaux est essentielle pour la monnaie *bitcoins*, qui n'est gérée par aucun nœud central de réseau qui contrôlerait l'ensemble des communications. La transaction qui résulte des échanges entre Alice et Bernard sera publique (tous les ordinateurs présents sur le réseau y auront accès) et permettra la mise à jour par tous du cahier de comptes, qui indique combien de *bitcoins* sont déposés dans chaque porte-monnaie existant.

- Alice souhaite envoyer N *bitcoins* à Bernard.
- Bernard communique sa clef publique B_{pub} à Alice.
- Alice forge un message M de transaction contenant la clef publique B_{pub} de Bernard et la somme N à transférer : $M = B_{pub}\, N$.
- Alice signe la transaction M avec sa clef privée A_{pri}, c'est-à-dire calcule une suite de symboles $M' = f(A_{pri}, M)$ qui, avec sa clef publique A_{pub}, redonne M : $g(A_{pub}, M') = M$ (tout le monde peut donc contrôler que c'est Alice qui a signé, mais personne ne peut signer à sa place).
- Alice diffuse la transaction signée sur le réseau afin qu'elle soit vue par tout le monde. Le protocole réel est légèrement plus compliqué (il contrôle qu'Alice dispose bien de la somme N dans son porte-monnaie).

En regardant cette transaction depuis l'extérieur, tout le monde voit que l'individu qui contrôle le compte d'Alice (individu que personne ne connaît) a donné son accord pour transférer N *bitcoins* sur le compte contrôlé par l'individu Bernard (que nul ne connaît).

Ne disposant pas de la clef privée d'Alice, personne d'autre qu'elle ne peut envoyer une telle transaction sur le réseau. Son envoi est donc la preuve qu'Alice était d'accord pour le transfert. Tout le monde considérera alors le transfert comme valide.

Le protocole de signature à doubles clefs utilisé est considéré comme robuste. Bien sûr, s'il venait à être cassé (c'est-à-dire si, par exemple, on réussissait à trouver une méthode rapide pour calculer la clef privée à partir de la clef publique), tout le système de la monnaie *bitcoin* s'effondrerait.