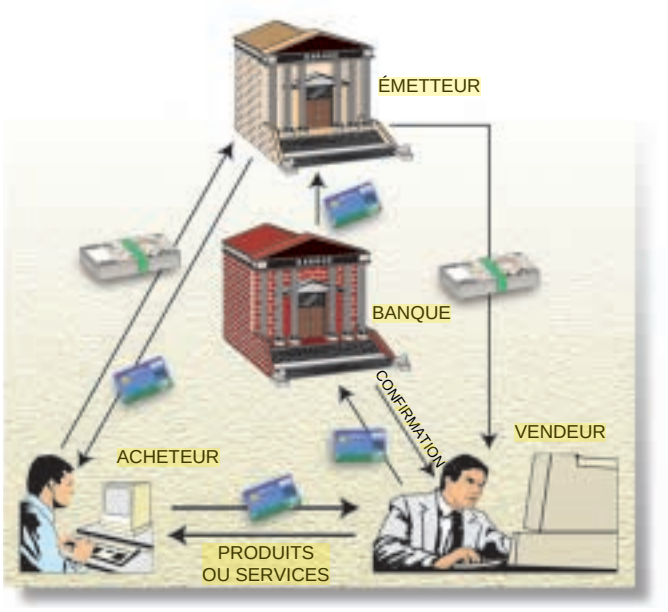
Ces représentations monétaires sont échangées à l'aide de systèmes transactionnels qui doivent empêcher l'accès non autorisé aux données – et aux fonds – privées des utilisateurs. Le chiffrement et le contrôle d'accès, tel le mot de passe, protègent relativement bien contre ce type d'intrusion. En revanche, le problème des «dépenses multiples» est plus ardu : comment s'assure-t-on qu'un billet virtuel n'a pas été copié plusieurs fois et dépensé auprès de différents vendeurs de façon illicite? Aujourd'hui, on effectue le contrôle en utilisant le numéro de série du billet et des coordonnées des utilisateurs des billets, qui sont toujours inclus dans les protocoles de paiement au moyen d'argent virtuel. L'émetteur du billet dissuade ainsi les fraudeurs putatifs, qui peuvent être retrouvés. Toutefois, dans les systèmes classiques, aucune donnée n'est fournie sur l'historique du billet ou sur sa date d'expiration.

Récemment, des informaticiens de la Société *Digital* ont introduit le concept de micropaiement. Ce système, nommé *MilliCent*, utilise des «coupons virtuels» qui abaissent le montant minimal d'une transaction. Tout comme les coupons de réduction dans le «monde réel», ces coupons ne sont utilisables qu'auprès de leur magasin émetteur. Des paiements de quelques centimes sont ainsi possibles. Ce type de transactions ouvre des nouvelles possibilités : les entreprises pourraient faire payer la recherche d'une information, comme une cotation boursière par exemple.



1. LES SYSTÈMES DE PAIEMENT CLASSIQUES nécessitent en général quatre acteurs. L'acheteur achète des biens et des services à l'aide d'une représentation monétaire (carte de crédit virtuelle, chèque électronique, argent virtuel, etc.). Le vendeur est crédité de la somme correspondante par l'émetteur de la représentation monétaire, après vérification par une banque ou par un intermédiaire. La sécurité de la transaction dépend de la représentation monétaire et du type de vérification.

La transaction

Comment s'effectue une transaction numérique? Plusieurs acteurs y participent : un acheteur, qui désire échanger son argent contre des biens ou des services offerts en ligne ; le vendeur, qui offre ces biens ou ces services ; un intermédiaire, ou courtier virtuel, qui traite les transactions ; une banque, qui gère les comptes des clients et acquitte les transactions ; enfin un émetteur – généralement une banque –, qui émet la représentation monétaire utilisée dans le système, qui protège la qualité de cette représentation monétaire, et, ainsi, les valeurs qu'elle représente.

Par exemple, dans le monde réel, la représentation monétaire émise par la *Deutsche Bundesbank* est le Deutsche Mark qui a, selon les analystes financiers, une qualité supérieure à celle du rouble russe ou du peso chilien ; cette qualité supérieure résulte non seulement d'une très bonne qualité d'impression et de l'utilisation d'un bon papier, mais surtout du fait que cette représentation monétaire est émise par une institution qui inspire confiance.

De façon générale, un client envoie la représentation monétaire chez un vendeur, qui la vérifie en l'envoyant à l'intermédiaire ou directement à la banque. Selon le résultat de cette vérification, le vendeur reçoit – le cas échéant – une confirmation et envoie alors la marchandise au client. L'acheteur achète cette représentation monétaire auprès de l'émetteur, qui peut aussi rembourser le vendeur *(voir la figure 1)*.

L'évaluation du paiement

Au vu du nombre croissant de systèmes numériques de paiement, leur évaluation est primordiale pour tous ceux qui veulent déployer et utiliser de tels systèmes transactionnels. Pour ce faire, nous avons proposé une taxonomie des systèmes de paiement numérique sur l'Internet.

Dans notre classification, les systèmes se divisent en deux grandes catégories, suivant que le système requiert ou non une adhésion de l'acheteur. Chacune des deux catégories contient plusieurs classes selon le modèle transactionnel et le niveau de protection – par exemple, le modèle sans protection, le modèle «débit-crédit», le modèle comptant, etc. Chaque classe contient un ou plusieurs groupes de systèmes de paiement reflétant la technique de transfert de fonds employée – par exemple, les systèmes fondés sur les mots de passe, les chèques électroniques, la facturation et les cartes de crédit, l'argent virtuel, etc.

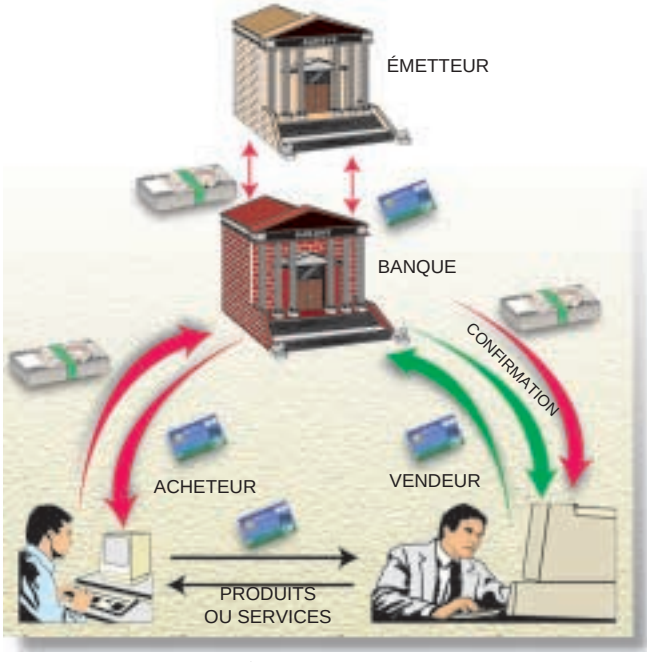
Comment évaluer les systèmes transactionnels? À l'aide de leurs caractéristiques. On distingue les caractéristiques internes, liées au fonctionnement intrinsèque du système, et les caractéristiques externes. Les caractéristiques internes sont la sécurité, la représentation monétaire, la pérennité de cette représentation, sa «granularité» (la plus petite somme que l'on peut échanger, surtout importante pour les micropaiements), la configuration du système et le niveau d'anonymat. Dans les caractéristiques externes, on inclut des critères tels que le délai d'encaissement, le mode d'échange des fonds ou la convertibilité de la représentation monétaire.

Aujourd'hui, le protocole de sécurisation des communications transactionnelles le plus répandu est le protocole SSL (*Secure Socket Layer*, soit «couche de base sécurisée»). Introduit en 1994 par la Société *Netscape Communications*, ce protocole est intégré dans les navigateurs les plus courants, tels *Netscape Navigator* et *Microsoft Internet Explorer*. Ce système est relativement sûr : en Europe, le protocole SSL chiffre les données avec des clés de 40 bits. Autrement dit, pour percer le code de chiffrement, il faudrait trouver les facteurs premiers d'un nombre de 40 bits (ou 10 chiffres), ce qui prendrait des jours à un ordinateur de bureau.

Pour les utilisateurs équipés de ces navigateurs, le chiffrement est transparent : lorsqu'un utilisateur entre son numéro de carte bancaire sur un site sécurisé (reconnaissable à l'adresse Web, où *http* est changé en *https*), celui-ci est chiffré automatiquement par l'ordinateur de l'utilisateur, puis il transite sur le réseau et il est décrypté par la machine du serveur. Cette ergonomie explique la percée de ce système, mais l'utilisation des cartes de crédit réelles restreint son usage à ceux qui en détiennent. De surcroît, avec les cartes de crédit, seuls les montants supérieurs à 50 francs sont économiquement viables, de sorte que ce système n'est pas intéressant pour l'achat d'articles de journaux en ligne, par exemple.

Autres restrictions de ce système transactionnel, il n'offre pas la non-répudiation (un usager pourrait prétendre ne pas être celui qui a fait la commande), et seule la communication est protégée : l'accès aux informations transactionnelles – notamment aux numéros des cartes de crédit utilisées – étant accessible aux vendeurs et aux intermédiaires, le niveau de sécurité de ce système est considéré comme moyen. Notons cependant que l'achat dans une boutique à l'aide d'une carte de crédit possède un niveau de sécurité analogue : la facturette où figure votre numéro de carte et sa date d'expiration est également accessible au vendeur.

Le système de paiement proposé par la Société *CyberCash* corrige certaines faiblesses du protocole SSL par l'ajout d'un «porte-monnaie électronique». De cette manière, *CyberCash* assure l'authentification des intervenants et un niveau raisonnable de non-répudiation des transactions, aspect totalement absent de SSL, qui n'est qu'un protocole cryptographique utilisé pour sécuriser les communications. La solution française *Klebox* possède des caractéristiques analogues.



2. AVANT UN PAIEMENT À L'AIDE DE *TRANZIX*, l'acheteur achète de l'argent numérique. L'acheteur clique sur un lien dans un magasin virtuel. Le portefeuille virtuel du vendeur contacte alors celui de l'acheteur en lui envoyant une requête de paiement pour la marchandise demandée. Lorsque le paiement est approuvé par l'acheteur, le vendeur reçoit un ou plusieurs billets numériques qu'il peut déposer immédiatement à la banque afin de vérifier leur validité, prévenant ainsi toute tentative de dépenses multiples. Le vendeur peut faire les vérifications hors ligne *(les flèches vertes représentent des transactions qui se font en ligne ou hors ligne ; les flèches rouges représentent des transactions hors ligne et les flèches noires des transactions en ligne)*.

Les cartes à puce

Les cartes à puce sont bien connues en Europe depuis près de 20 ans. Utilisées principalement comme cartes bancaires et téléphoniques, elles trouvent une nouvelle utilisation comme moyen ergonomique de paiement sur l'Internet. La Société britannique *Mondex* va permettre l'utilisation sur l'Internet de sa carte de paiement : à l'aide de lecteurs spécifiques branchés sur un port de communication d'un ordinateur, deux cartes *Mondex* effectueront des transactions sécuritaires. Le niveau de sécurité de ce système est élevé. La disponibilité, l'intégrité, la confidentialité et l'authentification sont assurées par des techniques cryptographiques. Seul le critère de non-répudiation n'est pas respecté, car un usager pourrait prétendre ne pas être celui qui a effectué la commande. Si les projets pilotes sont des succès, cette méthode sera généralisée à des transactions à l'aide de cartes à puce classiques.

Un niveau de sécurité encore supérieur a été mis au point par la Société hollandaise *DigiCash*. Le système, nommé *eCash*, utilise le concept d'argent électronique pour le paiement sur l'Internet. Il s'agit de pièces de monnaie virtuelles que l'on achète avec de l'argent réel (moyennant un transfert bancaire par exemple) et que l'on échange à chaque achat contre des produits et des services. Une méthode de chiffrement asymétrique assure la disponibilité et la confidentialité de l'information, et un système de signatures numériques assure l'intégrité de l'information, l'authentification des intervenants et la non-répudiation des transactions. De surcroît, le système permet des paiements anonymes grâce au concept de la signature aveugle : le numéro de série d'une pièce électronique est «caché» avant que la banque ne le signe, à l'aide d'un «facteur d'aveuglement» avec lequel ce numéro sera multiplié arithmétiquement.

Pour les micropaiements, même si plusieurs systèmes ont été proposés récemment, seul *MilliCent*, mis au point par la Société *Digital*, a dépassé la phase de recherche. Aujourd'hui en phase de tests, il permet le paiement de montants de quelques centimes à l'aide de coupons émis par chaque vendeur. Les coupons sont achetés et échangés auprès de courtiers virtuels.

Transactions généralisées

En analysant tous ces systèmes, nous avons déterminé les besoins à combler. Nous avons alors proposé un nouveau système transactionnel qui autorise le transport de valeurs numériques sans restrictions sur leur nature intrinsèque.

Bien qu'ils varient par la manière dont ils effectuent une transaction, tous les systèmes actuels ne font qu'une seule opération : un paiement électronique. Pour étendre cette fonction, nous avons mis au point le système *TRANZIX*, qui ouvre la porte à toute autre transaction, tels le transport, le transfert ou l'échange de valeurs. La notion de valeur généralise le concept de paiement.