Université de Montréal

Les procédés cryptographiques de monnaie électronique : design, fonctionnalités et usages

par

Jean-François Blanchette

Département d'informatique et de recherche opérationnelle
Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de
Maître ès sciences (M.Sc.)
en Informatique

4 octobre 1997

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé

Les procédés cryptographiques de monnaie électronique : design, fonctionnalités et usages

présenté par :

Jean-François Blanchette

a été évalué par un jury composé des personnes suivantes :

(président-rapporteur)
François MAJOR

(directeur de recherche)
Claude CRÉPEAU

(membre du jury)
Gilles BRASSARD

Mémoire accepté le :

Sommaire

Ce mémoire traite du design de produits de haute technologie, issus de la science cryptologique : les procédés de monnaie électronique. La monnaie électronique se prépare à faire irruption au sein de nos vies, en tant que mécanisme de paiement destiné à remplacer la monnaie de métal et le papier-monnaie ; c'est dire que cette technologie s'insère au sein d'un réseau touffu de pratiques sociales, légales, historiques et politiques. Il apparaît donc pertinent de s'intéresser au processus par lequel cette technologie acquièrt les fonctionnalités qui lui sont propres ainsi qu'aux acteurs appelés à participer à l'entreprise de design.

Il est pourtant difficile d'identifier un tel processus : le discours dominant qui accompagne l'introduction de nouvelles technologies au sein de nos sociétés ne s'écarte que rarement des ornières de l'idéologie techniciste, qui veut que le progrès technologique soit non seulement inévitable, mais également nécessairement orienté dans le sens du progrès humain. Un tel discours tend à occulter la complexité des relations qui nous unissent aux objets techniques et surtout, les jeux de pouvoir et d'influence qui résultent en une forme donnée d'un objet technologique. La socio-politique des usages se préoccupe d'offrir une alternative à ce discours, par l'analyse des logiques techniques, économiques et sociales, qui à elles trois déterminent les *usages* d'un artefact technologique donné.

Nous effectuons donc le survol des possibilités techniques offertes par les procédés de monnaie électronique, en tentant de dégager les principaux acteurs influençant le processus de recherche. À cet effet, nous procédons à une analyse exhaustive de la littérature scientifique et exposons de façon cohérente et structurée les concepts clés de même que les différentes fonctionnalités — divers degrés de protection de la vie privée, divisibilité, transférabilité, micropaiements — qui caractérisent les solutions cryptographiques au problème du paiement électronique. Pour conclure, nous examinons différentes approches critiques du processus de design de ces artefacts.

Mots clés : Cryptologie, monnaie électronique, socio-politique des usages, design, innovation technologique.

Table des matières

Identification du jury i

Sommaire ii

Mots clés ii

1 Introduction 1

1.1 La socio-politique des usages 2

1.2 Organisation des chapitres 4

2 Préliminaires cryptographiques 6

2.1 Protocoles et entités 7

2.2 Saveurs de sécurité 8

2.3 Problèmes réputés difficiles 8

2.3.1 La factorisation des entiers 9

2.3.2 RSA 9

2.3.3 Le calcul du logarithme discret 9

2.3.4 Le calcul d'une représentation 10

2.4 Preuves interactives 10

2.4.1 Démontrer la possession d'une représentation 10

2.5 Fonctions de hachage 11

2.6 Cryptosystèmes 12

2.6.1 Cryptosystèmes à clé secrète 13

2.6.2 Cryptosystèmes à clé publique 13

2.6.3 Cryptosystème RSA 13

2.7 Signature numérique 14

2.7.1 Attaques sur les procédés de signature numérique 15

2.7.2 Procédé de signature numérique RSA 15
2.7.3 Procédé de signature numérique de Chaum-Pedersen 15

3 Fondements de la monnaie électronique **18**
3.1 Modèle 20
3.2 Entités 21
3.3 Bidules 22
3.4 Fonctionnalités 23
3.4.1 Protocoles 23
3.4.2 Transférabilité et divisibilité 24
3.4.3 Robustesse 24
3.5 Structure 24
3.6 Sécurité 25
3.6.1 Attaques 25
3.6.2 Hypothèses de fiabilité 27
3.6.3 Résilience 28
3.7 Vie privée 28
3.8 Armature 28

4 Protection de la vie privée **31**
4.1 Réseaux anonymes 32
4.2 Signatures à l'aveugle 34
4.2.1 À la Chaum 35
4.2.2 À la Chaum-Pedersen 36
4.3 Un second procédé 37

5 La détection de la réutilisation **40**
5.1 L'encodage de l'identité 41
5.2 Signature à l'aveugle restrictive 42
5.2.1 Ouverture d'un compte 43
5.2.2 Protocole de retrait 43
5.2.3 Protocole d'achat et de dépôt 45

6 Portefeuilles avec observateurs **47**
6.1 Dispositifs pour un portefeuille électronique 48

6.1.1 Ordinateur 48
6.1.2 Module inviolable 49
6.1.3 Portefeuille électronique avec observateur 49
6.2 Protocoles 50

7 Révocabilité 53
7.1 Protocoles pour un procédé révocable 56
7.1.1 Identifier un individu 58
7.1.2 Identifier une pièce 59

8 Divisibilité et transférabilité 60
8.1 Transférabilité 61
8.1.1 Ajouter la transférabilité 61
8.2 Divisibilité 64
8.2.1 La technique d'Okamoto 65
8.2.2 Calcul des valeurs de chaque nœud 66
8.2.3 Retrait d'une pièce 66
8.2.4 Protocole de paiement 67
8.3 Autres approches 68

9 Les micropaiements 70
9.1 Protocoles 71
9.1.1 Paiement 72
9.1.2 Protocole de dépôt 73

10 Conclusion 75
10.1 De l'usager 78

Références 81

Table des figures

2.1 Notation pour les protocoles interactifs 7
2.2 Démontrer la possession d'une représentation 11
2.3 Preuve interactive que $\log_g y = \log_m z$ 16

3.1 Procédé de base : protocole de retrait 29
3.2 Procédé de base : protocole d'achat 29
3.3 Procédé de base : protocole de dépôt 29

4.1 Signature à l'aveugle à la Chaum 35
4.2 Signature à l'aveugle à la Chaum-Pedersen 37
4.3 Procédé anonyme : protocole de retrait 38
4.4 Procédé anonyme : protocole d'achat 38
4.5 Procédé anonyme : protocole de dépôt 38

5.1 Procédé de Brands : ouverture de compte 43
5.2 Procédé de Brands : protocole de retrait 44
5.3 Procédé de Brands : protocole d'achat 45

6.1 Procédé avec observateur : ouverture d'un compte 50
6.2 Procédé avec observateur : protocole de retrait 51
6.3 Procédé avec observateur : protocole d'achat 52

7.1 Procédé révocable : initialisation du système par le fiduciaire 56
7.2 Procédé révocable : protocole de retrait 57
7.3 Procédé révocable : protocole d'achat 58
7.4 Procédé révocable : retracer un individu avec l'aide du fiduciaire 59
7.5 Procédé révocable : retracer une pièce avec l'aide du fiduciaire 59

8.1 Transfert d'une pièce entre deux utilisateurs 62
8.2 Procédé transférable : protocole de paiement 63
8.3 Structure d'une pièce divisible 65

9.1 Procédé de micropaiements : paiement du i^e tic 73
9.2 Procédé de micropaiements : protocole de dépôt 74

Dédié affectueusement à la mémoire de ma grand-mère, Alvine MERCIER,
née le 10 mars 1911, décédée le 25 décembre 1992.

Avant-propos

« Writing is easy. All you do is stare at a blank sheet of paper until drops of blood form on your forehead. »
GENE FOWLER

Mes études scientifiques, si elles furent l'occasion d'un enrichissement intellectuel certain, ont été caractérisées par une certaine ambivalence : le plaisir tangible éprouvé à l'exploration des paysages mathématiques dénudés — inhospitaliers, diraient certains — de l'informatique théorique s'est en effet trouvé tempéré par un questionnement d'ordre plus moral sur la place prépondérante qu'occupe la vision scientifique et le fait technologique en tant que modes d'exploration et de manipulation de notre univers physique.

Il semble pertinent de nos jours de rapprocher ces deux questionnements : comme le souligne l'anthropologue Shosana ZUBOFF (1988), les technologies résultant de la science informatique effectuent une réorganisation fondamentale de l'infrastructure matérielle de notre monde et, par ce fait, de la texture même de l'univers politique et social qui en dépend.

Au sein du curriculum universitaire, de telles pistes de réflexion sont encore largement absentes : à notre époque, l'argument économique — épaulé de son fier-à-bras, la mondialisation des marchés — représente la finalité suprême et justification unique de la coupe à blanc sociale caractéristique de l'implantation de nouvelles technologies. La mission universitaire, réduite à sa plus simple expression de formation utilitaire, se satisfait de bêtement débiter la chair à canon — dûment diplômée — de l'ère de l'information, dernier dada des millénaristes technologiques. Là où les idéaux de la recherche fondamentale ont pu échapper aux prosélytes de la collaboration industrielle, la réflexion se limite généralement à une profession de bons sentiments, sous la houlette paternelle d'universitaires en fin de carrière. [1]

Pourtant, comme toute autre activité humaine, le processus de découverte scientifique et de développement technologique est sujet à l'étude et à l'investigation. La cryptologie se présente à cet égard comme un terroir particulièrement fertile, s'employant à la translation d'artefacts caractéristiquement *low-tech* — papier-monnaie, signature manuscrite — en de purs produits *hi-tech* — cartes à puce, signature numérique. De tels artefacts sont si profondément, et depuis si longtemps, mêlés à nos pratiques sociales qu'il paraît légitime de se demander si leur numérisation correspond à un simple déplacement sur un nouveau support ou résulte plutôt en un outil dont les modalités ne nous sont que superficiellement connues.

On aura compris que l'objectif de ce mémoire n'est pas la production de résultats scientifiques originaux propres à faire progresser la recherche fondamentale en cryptologie. Il s'agit plutôt d'une tentative de dégager quelques pistes qui puissent nous être utiles à préciser la nature des changements que préfigurent les technologies cryptographiques. Du côté scientifique, je me suis appliqué à la maîtrise du langage hermétique caractéristique de la cryptologie [2], à l'acquisition des notions fondamentales de cette science de même qu'au développement de ma capacité à les vulgariser. Mes incursions sociologiques ont voulu établir quelques approches possibles à l'étude et à la compréhension du processus par lequel des artefacts technologiques tels que la monnaie électronique acquièrent leur forme. Le tout constituera — c'est mon espoir — une fondation adéquate à des études doctorales consacrées à une exploration plus approfondie de techniques qui exercent leur action au cœur même du tissu social.

* * *

Mon séjour à l'Université de Montréal aura été l'occasion d'une renaissance académique personnelle, dont j'aimerais chaleureusement remercier certains des acteurs : chez les professeurs, mon directeur de recherche, Claude Crépeau, a patiemment accepté de partager un cheminement parfois tortueux ; Gilles Brassard, Marc Feeley, Michael J. Ferguson, Christian Léger, Jacques Malenfant ainsi que Pierre McKenzie ont su doublement m'inspirer, tant par leur enseignement que par leur professionnalisme ; Daniel Poulin a eu la gentillesse de rédiger une quantité astronomique de lettres de recommandation. Chez les étudiants, André Berthiaume a, le premier, suggéré que je

1. « *And out comes the after-dinner speaker, an old trooper, usually a distinguished scientist or engineer, often someone who helped pioneer an advanced weapons system of some sort, to address his colleagues on "technology and human values".* » (WINNER 1986)

2. De l'opinion de deux mathématiciens, DAVIS et HERSH (1981), « [...] *computer science in its theoretical formulation is dominated by a spirit of abstraction which defers to no other branch of mathematics in its zealotry.* »

puisse trouver ma place au sein du laboratoire d'informatique théorique ; Augustin Baziramwabo, Samy Bengio, Jeroen van de Graaf et Alexandre Guimond m'ont fait sentir un des leurs. Maddy Kieffer, Carole Paradis et tout le personnel de la bibliothèque ont su me fournir un support tant documentaire que moral. Gabrielle Caron, Francois Guénette, Monique et Normand Lapointe, Vincent Morinville, Pierre Patenaude, Carlos Ponce et mon valeureux grand-père, Alban Blanchette, ont fait de leur mieux pour me détourner de la rédaction de ce mémoire lorsque c'était nécessaire. Le Conseil de recherches en sciences naturelles et en génie du Canada m'a permis, grâce à son aide généreuse, de me consacrer (presque) exclusivement à l'étude. Luce Des Marais a scruté de son œil expert et maniaque les épreuves finales ce mémoire, les bénissant sans retenue de sa plume rouge.

J'aimerais remercier tout particulièrement Paul Bratley, mes bonnes amies Danièle Bourque et Ariane Lazaridès ainsi que mon collègue Alain Tapp : leur foi apparemment inébranlable en mes capacités s'est finalement révélée plus difficile à vaincre que mes propres doutes.

Chapitre 1

Introduction

> « *Is e-money really going to happen ? Inevitably. Hard currency has been a useful item for a few millenia or so, but now it has simply worn out its welcome.* »

Cette citation (LEVY 1994), tirée de *Wired*, un magazine voué à la promotion du phénomène informatique, est typique du discours simpliste généralement utilisé pour décrire un des événements dominants de notre époque : la numérisation d'un grand nombre d'artefacts matériels — dont la monnaie — auxquels sont intimement liés plusieurs comportements sociaux. S'articulant simultanément sur les deux axes de l'*inévitabilité* du fait technologique de même que son avancée inexorable dans le sens du *progrès* humain, ce discours s'accompagne généralement d'un regard condescendant sur des objets — livre, signature, papier-monnaie — pourtant assez robustes pour traverser tant les époques que les civilisations. Cette attitude a pour effet d'occulter le réseau complexe de relations sociales au cœur duquel les technologies numériques se trouvent littéralement parachutées et de limiter ainsi considérablement les discussions qui pourraient survenir au cours de leur introduction au sein de nos sociétés.

Ce mémoire a pour objectif de dégager quelques avenues possibles de recherche concernant le processus par lequel les technologies prennent forme pour finalement aboutir entre les mains des utilisateurs. Notre approche tente de demeurer à l'écart des ornières du discours techniciste qui nous aveugle aux démarches complexes de négociation par lesquelles émergent les artefacts technologiques. Il nous semble particulièrement important de pouvoir éclairer ces processus, dans la mesure où les technologies issues de la science cryptologique s'apprêtent à faire irruption au cœur même de notre quotidien. La cryptologie offre en effet la possibilité d'automatiser des catégories entièrement nouvelles de fonctions sociales, telles la non-répudiation (par le biais de la signature) et l'échange de biens et services (par le biais de la monnaie). Les technologies utilisées à cet effet sont restées essentiellement inchangées durant des siècles : la monnaie de métal, le papier-monnaie, la signature manuscrite se sont révélés des outils étonnamment flexibles, robustes et adaptables, à travers le temps et l'espace. Il semble donc approprié de s'interroger sur leur éventuel remplacement par de nouvelles façons de faire, dont bien peu de choses nous sont encore connues.

1.1 La socio-politique des usages

Étonnamment, il paraît parfois difficile de nos jours d'approfondir ces interrogations, pourtant légitimes. Le vocabulaire, les concepts, les catégories qui pourraient nous permettre d'amorcer une telle réflexion semblent curieusement absents. Le processus d'innovation technologique semble affligé d'une amnésie historique chronique, que viennent timidement critiquer les traditionnelles constatations des dommages *après-coup*, sous leur forme d'études d'impacts sociaux. Il existe pourtant une riche tradition de recherche qui s'est consacrée à ce qui est certainement l'une des marques constitutives de l'époque moderne, c'est-à-dire la place prépondérante qu'ont acquise les sciences et les technologies au sein de nos vies, de même que les modes d'appréhension et de structuration du réel qu'elles induisent. [1] Cependant, le champ de ce qui est communément désigné par les « études des sciences et des technologies » [2] présente un paysage inégal, difficilement catégorisable, aux fondations encore mal établies. Au sein des grands courants de pensée qui structurent le domaine, se distingue une approche syncrétique qui nous semble particulièrement prometteuse, dite de la socio-politique des usages [3], c'est-à-dire qu'elle est centrée sur *les usagers et leurs utilisations des technologies*. Comment cette approche peut-elle nous être utile ? Selon PROULX (1994),

> « *Avec d'autres chercheurs, je crois que l'une des pistes possibles consiste dans la réalisation d'études concrètes se donnant pour objectif la description méticuleuse et fine — dans toute leur complexité — des multiples rapports de médiation unissant les usagers aux objets techniques. Cette perspective permettrait la mise à jour des multiples chaînes de médiations articulant les rapports d'usage aux micro-contextes (vie quotidienne, dynamique familiale) et aux macro-contextes.* »

En d'autres termes, les objets techniques profitent d'être examinés non seulement en fonction des objectifs explicites qui ont guidé leurs concepteurs, mais également en fonction des appropriations, voulues ou non, qu'en font leurs utilisateurs.

Certains phénomènes issus de l'innovation technologique ont déjà fait l'objet de telles études : Siegfried Giedion (GIEDION 1948), par exemple, s'est penché sur le pro-

1. Le lecteur intéressé se référera aux ouvrages de WINNER (1977) et VEDEL (1994) pour des introductions plus fouillées à ce sujet.
2. *Science and Technology Studies (STS).*
3. *Uses and gratifications.*

cessus de mécanisation de l'effort humain, en examinant entre autres ses effets sur le métier de serrurier, l'industrie de l'agriculture, la fabrication du pain, le design des meubles, les tâches ménagères et la salle de bain. Dans le même esprit, David Nye a examiné le processus de l'électrification aux États-Unis (NYE 1990), un événement technologique dont l'impact sur nos vies quotidiennes peut difficilement être nié.

Dans le contexte des artefacts qui nous intéressent — ceux issus de la science cryptologique — une telle démarche excède évidemment de beaucoup le cadre d'un mémoire de maîtrise, tant sur le plan des ressources matérielles et documentaires nous étant accessibles que sur celui des nos compétences actuelles de chercheur. La portée de nos recherches se limitera donc à une exploration des caractéristiques techniques de la monnaie électronique. Cette détermination des possibilités représente néanmoins un élément essentiel à notre compréhension puisque, comme le souligne VITALIS (1994) :

> « [. . .] *pour faire apparaître tous les enjeux et notamment les enjeux socio-politiques, il convient de situer l'usage au carrefour de trois logiques principales : une logique technique qui définit le champ des possibles, une logique économique qui détermine le champ des utilisations rentables et une logique sociale qui détermine la position particulière de l'usager avec ses besoins et ses désirs. Chaque logique a ses moyens d'expression et c'est leur interaction qui va donner vie aux usages observés dans la pratique.* »

Les contraintes inhérentes à l'objet technique ne se situent pas uniquement au niveau des possibilités qu'il offre ou n'offre pas, mais incluent également les compétences qu'il nécessite, et le degré de difficulté avec lequel celles-ci peuvent être acquises.

Voilà précisément où nous avons voulu situer la contribution originale de ce mémoire. Cette définition des possibles techniques se révèle pourtant plus difficile qu'il ne pourrait le sembler à première vue. La communication scientifique, sous sa forme contemporaine, tend à obscurcir considérablement le processus de design [4] : les résultats, émergeant de l'éther mathématique, sont généralement présentés sans la moindre référence au contexte social, politique et historique qui les motivent et les justifient. Au-delà des résultats scientifiques, notre objectif est donc de synthétiser la littérature de façon à faire ressortir le *processus de design* de la monnaie électronique, c'est-à-dire :

1° De pouvoir apprécier le déroulement historique de la démarche, jusqu'à son aboutissement à l'état de l'art actuel ;

2° De disposer d'une vue d'ensemble cohérente des possibilités actuelles offertes par la monnaie électronique ;

4. Cela est en partie dû à une certaine conception du style scientifique — « *The accepted from of "objectivity" in scientific and technical reports (one can also include books and articles in social science) requires that the prose read as if there were no person in the room when the writing took place.* » (WINNER 1986) qui a pour effect d'occulter ainsi les motivations et orientations de la recherche.

3º De disposer d'une présentation unifiée des principaux résultats, tant du point de vue de la notation et de la terminologie que des concepts fondamentaux ;

4º D'effectuer une présentation vulgarisée de concepts qui tendent à n'être accessibles qu'à un public restreint d'initiés ;

5º D'offrir un parcours guidé de la littérature essentielle traitant des procédés cryptographiques de monnaie électronique ;

6º D'offrir quelques pistes de réflexion quant aux problématiques socio-politiques que soulève l'utilisation de la monnaie électronique.

J'ai espoir que cette contribution formera une fondation adéquate à de futures études doctorales, où ces problématiques seront l'objet de considérations plus approfondies.

1.2 Organisation des chapitres

Ce mémoire se veut sujet à deux lectures possibles : une première, plus superficielle, évitera les descriptions mathématiques des protocoles mais permettra néanmoins de s'initier aux différentes problématiques techniques afférentes à la monnaie électronique et d'apprécier les apports des différents protagonistes actifs au sein du processus de design. Une seconde, plus complète, permettra à un public initié aux rudiments de la cryptologie d'acquérir ou de mettre à jour les notions théoriques fondamentales touchant aux procédés cryptographiques de monnaie électronique.

L'organisation des chapitres tente de refléter l'évolution de la recherche dans le domaine : les chapitres 2 et 3 sont l'occasion de nous munir, d'une part, des blocs cryptologiques dont sont constitués les procédés de monnaie d'autre part, d'une exposition détaillée de la problématique du paiement électronique de même que des caractéristiques essentielles de la monnaie électronique.

Historiquement, la protection de la vie privée a été une des problématiques principales ayant motivé la recherche, et la présentation des solutions techniques qui ont tenté d'y répondre occupe les chapitres 4 et 5. Cette protection se présente cependant sous différents modèles, offrant tant aux organisations qu'aux individus des assurances de sécurité variables : ces modèles forment l'objet des chapitres 6 et 7.

D'autres considérations plus prosaïques viennent aussi largement définir le champ des utilisations possibles de la monnaie électronique : la capacité à effectuer des paiements entre particuliers ainsi que les difficultés techniques que présente la nécessité de pouvoir effectuer des paiements de valeur variable de façon efficace constitue l'essentiel du chapitre 8. Dans le même ordre d'idées, le chapitre 9 se consacre à une forme restreinte de la monnaie électronique, le micropaiement, qui semble promis à une carrière brillante depuis que le développement sans précédent des réseaux électroniques internationaux fait entrevoir l'émergence de vastes marchés pour l'acquisition de contenu à faible coût.

Comment nous est-il possible de juger de la qualité des différentes solutions qui nous sont proposées pour remplacer le papier-monnaie ? La littérature scientifique ne retient généralement que les critères d'efficacité et d'élégance mathématique, mais ceux-ci se révèlent inadéquats face à un objet aussi socialement complexe et multiforme que la monnaie. En guise de conclusion, le chapitre 10 propose donc quelques critères qui puissent nous guider dans notre quête d'un substitut numérique aux espèces sonnantes et trébuchantes. Une forme du processus de design, plus à même de produire des objets techniques satisfaisant à ces critères, est aussi évoquée. Une bibliographie fouillée de la littérature complète ce mémoire. [5]

* * *

Avant toute chose, il importe de disposer d'une solide compréhension des concepts fondamentaux de la cryptologie de même que des outils spécifiques pertinents à notre propos : c'est l'objet du prochain chapitre.

5. Il est possible d'accéder en ligne à plusieurs des documents cités dans ce mémoire en consultant <http://www.iro.umontreal.ca/~blanchej/biblio.html>.

Chapitre 2

Préliminaires cryptographiques

« *... il a très bon esprit, mais il n'est pas géomètre ...* »
PASCAL, Lettre à FERMAT, 29 juillet 1654

La *cryptographie* est l'étude des méthodes mathématiques reliées à certains aspects de la sécurité de l'information, tels que la confidentialité, l'intégrité des données et la signature ; en général, la cryptographie ne représente qu'un seul des moyens nécessaires à la réalisation d'un objectif de sécurité spécifique. [1] De façon complémentaire, la *cryptanalyse* est l'étude des méthodes mathématiques à même de faire échouer ces objectifs ; la *cryptologie* [2] englobe à la fois cryptographie et cryptanalyse.

Un procédé cryptographique — cryptosystème, procédé de signature, procédé de monnaie électronique — se construit à partir de blocs fondamentaux, les *primitives cryptographiques*. Ces primitives se distinguent par les hypothèses calculatoires dont elles dépendent, leurs fonctionnalités, leur coût calculatoire et les objectifs de sécurité qu'elles permettent de réaliser. Ce chapitre présente un certain nombre de primitives pertinentes au contexte des procédés de monnaie électronique, de même que quelques notions fondamentales à l'étude des protocoles cryptographiques.

---

1. L'utilisation de méthodes cryptographiques n'est pas toujours indiquée : FAGIN, NAOR et WINKLER (1996) dressent une nomenclature amusante de solutions *low-tech* à un problème (l'évaluation de fonctions sur données privées) pour lequel on ne connaît que des solutions cryptographiques complexes.

2. Pour un survol historique de la cryptologie, on consultera KAHN (1967) ; pour une introduction générale à la cryptographie contemporaine, on consultera les ouvrages de RIVEST (1990), BRASSARD (1992), SIMMONS (1992), STINSON (1995) ainsi que MENEZES, VAN OORSCHOT et VANSTONE (1997).

2.1 Protocoles et entités

Un *protocole cryptographique interactif* est un algorithme distribué dans lequel une séquence d'étapes spécifie précisément les actions requises de deux ou plusieurs entités, dans le but d'atteindre un certain objectif de sécurité — confidentialité, signature, non-répudiation par exemple. Au sein d'un protocole cryptographique, une *entité* [3] est quelqu'un ou quelque chose qui envoie, reçoit ou manipule de l'information. [4]

Un protocole interactif $\langle \mathcal{A}(a), \mathcal{B}(b) \rangle$ pour les entités $\mathcal{A}$ et $\mathcal{B}$, disposant respectivement des entrées a et b, est dénoté par :

$\mathcal{A}(a)$		$\mathcal{B}(b)$
$\vdots$	$\xleftarrow{\text{communication}}$	$\vdots$
calculs privés		calculs privés
$\vdots$	$\xrightarrow{\text{communication}}$	$\vdots$
sortie/vue		sortie/vue

FIG. 2.1 - *Notation pour les protocoles interactifs*

La *vue* de $\mathcal{A}$ du protocole consiste en son entrée a, ses calculs privés, ses choix aléatoires, sa sortie ainsi que l'ensemble des messages échangés avec $\mathcal{B}$.

Un *adversaire* est une entité qui tente de faire échouer les objectifs de sécurité du protocole. On nomme *attaque* la stratégie utilisée à cet effet par l'adversaire ; si l'attaque réussit, on dira du protocole qu'il a été *brisé*. Les attaques sont généralement classifiées selon les ressources (calculatoires, matérielles ou autres) qu'elles exigent d'un adversaire.

3. Les entités seront notées $\mathcal{A}, \mathcal{B}, \ldots, \mathcal{Z}$.
4. La littérature désigne souvent par Alice une entité *émettrice*, source légitime d'information, et par Bob une entité *réceptrice*, destinataire légitime de cette information.

2.2 Saveurs de sécurité

Les protocoles et les primitives cryptographiques peuvent être évalués selon deux différents modèles de sécurité :

1° La sécurité *inconditionnelle*, où même un adversaire disposant de ressources calculatoires illimitées ne dispose pas de suffisamment d'information pour arriver à briser le système. Cette sécurité est évaluée dans le contexte de la théorie de l'information.

2° La sécurité *calculatoire*, où le calcul requis pour briser le système, même en utilisant les meilleures attaques connues, est perçu comme excédant — par une marge confortable — les ressources calculatoires d'un adversaire potentiel. Cette sécurité est évaluée dans le contexte de la théorie de la complexité calculatoire.

Les primitives offrant une sécurité calculatoire sont souvent reliées aux problèmes réputés difficiles (section 2.3). Lorsqu'une preuve d'équivalence à l'un de ces problèmes est connue, on parlera alors de sécurité *démontrable*, *i. e.* briser le système est équivalent à résoudre un problème réputé difficile. [5]

Ces cadres d'analyse demeurent des idéaux et, le plus souvent, les protocoles cryptographiques ne pourront offrir rien de mieux qu'une sécurité dite *heuristique*, [6] sécurité dont l'histoire de la cryptographie se charge de nous démontrer la fragilité. Il importe donc, autant que possible, de faire dépendre les protocoles cryptographiques d'hypothèses calculatoires connues.

2.3 Problèmes réputés difficiles

La sécurité des protocoles cryptographiques est généralement fondée sur la difficulté présumée [7] d'un petit nombre de problèmes, tirés pour la plupart de la théorie des nombres. [8] Une tâche calculatoire est *réputée difficile* si aucun algorithme permettant de

---

5. Si ces équivalences n'offrent pas, à proprement parler, d'assurances supplémentaires, elles ont le mérite de faire reposer la sécurité du procédé sur des hypothèses attentivement étudiées par la communauté scientifique.

6. BRANDS (1993) le souligne : « *However, the first mathematical proof of correctness of the existing* [cryptographic] *cash systems has yet to be given. In fact, all cash systems in literature have in common that they use such complicated constructions that almost nothing has been proven about their correctness, and intuitive arguments are given instead.* »

7. *Présumée*, car la complexité calculatoire de ces problèmes n'est pas connue.

8. Les principaux problèmes calculatoires pertinents à la cryptologie sont discutés dans MENEZES, VAN OORSCHOT et VANSTONE (1997), chap. 3.

l'effectuer en un temps [9] polynomial ne semble être connu ; sinon, elle est dite *facile*. Quatre de ces problèmes sont particulièrement pertinents à notre propos : la factorisation de grands entiers, le problème dit de RSA, le calcul de logarithmes discrets au sein d'un groupe fini et sa généralisation, le calcul de représentations. Dans chaque cas, nous spécifions les paramètres pour lesquels ces problèmes sont considérés difficiles, sans toutefois aller jusqu'à dresser la nomenclature exhaustive de leurs exemplaires faciles.

2.3.1 La factorisation des entiers

exemplaire : un entier positif n.

Problème : écrire n sous la forme $p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ où les p_i sont des entiers premiers distincts et $e_i \geq 1, 1 \leq i \leq k$.

Les plus récents exploits en matière de factorisation (LENSTRA 1996) ont révélés les facteurs premiers d'un n comportant 130 décimales.

2.3.2 RSA

exemplaire : deux nombres premiers impairs distincts p et q, un entier positif n tel que $n = pq$, un entier positif e tel que pgcd$(e, (p-1)(q-1)) = 1$ et un entier c.

Problème : déterminer un entier m tel que $m^e \equiv c \pmod{n}$.

Ce célèbre problème, dû à RIVEST, SHAMIR et ADLEMAN (1978), est réputé difficile si les facteurs p et q de n ne sont pas connus et s'il est difficile de factoriser n.

2.3.3 Le calcul du logarithme discret

exemplaire : G, un groupe fini cyclique d'ordre q, un générateur g de G et un élément $y \in G$.

Problème : déterminer l'unique entier x, noté $\log_g y$, tel que $g^x \equiv y \pmod{n}$, $0 \leq x \leq n-1$.

Le calcul d'un logarithme discret est réputé difficile pour un choix adéquat de l'ordre q de G ; en particulier, q devrait être un nombre premier d'au moins 150 décimales et $q - 1$ devrait comporter au moins un grand facteur premier.

9. Nous ne distinguons pas entre algorithmes déterministes au temps polynomial et algorithmes probabilistes au temps *espéré* polynomial.

2.3.4 Le calcul d'une représentation

Le problème de représentation peut être vu comme une généralisation du problème du logarithme discret :

exemplaire : un groupe G d'ordre q tel que le calcul de logarithmes discrets y est réputé difficile, k générateurs distincts $g_1, \ldots, g_k$ de G et un élément $h \in G$.

Problème : déterminer un k-tuple $(u_1, \ldots, u_k)$, $u_i \in \mathbb{Z}_q$, tel que $h = \prod_{i=1}^{k} g_i^{u_i}$, et qu'au moins un des $u_i \not\equiv 0 \pmod{n}$. Le k-tuple $(u_1, \ldots, u_k)$ est appelé une représentation de h par rapport aux générateurs $g_1, \ldots, g_k$.

Le problème de représentation est réputé difficile si, pour toute paire $(g_i, g_j), i \neq j$, le logarithme discret $\log_{g_i} g_j$ n'est pas connu. Dans le contexte des protocoles cryptographiques, cette difficulté nous permet de supposer que disposer d'une représentation $(u_1, \ldots, u_k)$ de h par rapport à k générateurs $g_1, \ldots, g_k$, aléatoirement choisis, est équivalent à avoir déterminé h en calculant $h = \prod_{i=1}^{k} g_i^{u_i}$.

2.4 Preuves interactives

Une preuve interactive est un protocole impliquant deux entités, $\mathcal{P}$ et $\mathcal{V}$, où $\mathcal{P}$ est en possession d'une certaine information et désire le démontrer à $\mathcal{V}$ sans toutefois lui communiquer directement cette information ; plus formellement, $\mathcal{P}$ veut convaincre $\mathcal{V}$ que x est un exemplaire positif d'un certain problème de décision Π, sans pourtant lui en exhiber la preuve.

Un protocole est défini comme une *preuve interactive pour* Π si, pour x un exemplaire positif de Π, un $\mathcal{V}$ honnête accepte toujours l'énoncé de $\mathcal{P}$ et si, pour x un exemplaire négatif de Π, un $\mathcal{V}$ honnête accepte l'énoncé de $\mathcal{P}$ avec une infime probabilité. Les preuves interactives sont classifiées selon la quantité d'information que $\mathcal{P}$ doit divulguer à $\mathcal{V}$ pour arriver à ses fins : dans une *preuve à divulgation nulle*,[10] $\mathcal{V}$ n'apprend strictement rien sur x, alors que les preuves interactives utilisées dans ce mémoire sont des *preuves à divulgation minimale*.[11]

2.4.1 Démontrer la possession d'une représentation

Le protocole de la figure 2.2 est une preuve interactive pour le problème de décision suivant :

10. *Zero-knowledge proof*.
11. *Minimum-disclosure proofs*.

exemplaire : un groupe G_q d'ordre premier q pour lequel le problème du logarithme discret est réputé difficile, k générateurs distincts $g_1, \ldots, g_k$ de G_q, k éléments $a_1, \ldots, a_k \in \mathbb{Z}_q$ et un élément $A \in G_q$.

Problème : $A \stackrel{?}{=} \prod_{i=1}^{k} g_i^{a_i}$.

$\mathcal{P}(g_1 \ldots g_k, a_1 \ldots a_k, A)$		$\mathcal{V}(g_1 \ldots g_k, A)$
$b_1 \ldots b_k \in_{\mathcal{R}} \mathbb{Z}_q$ $B \leftarrow \prod_{i=1}^{k} g_i^{b_i}$	$\xrightarrow{B}$	
		$d \in_{\mathcal{R}} \mathbb{Z}_q$
	$\xleftarrow{d}$	
for $i = 1$ **to** k **do** $r_i \leftarrow d \cdot a_i + b_i \bmod q$		
	$\xrightarrow{(r_1 \ldots r_k)}$	$\prod_{i=1}^{k} g_i^{r_i} = A^d \cdot B\,?$
		oui/non

FIG. 2.2 - *Démontrer la possession d'une représentation*

Si la représentation de B est fixée, plutôt que choisie aléatoirement pendant le protocole, celui-ci devient alors une preuve de possession de représentations de deux nombres par rapport au même générateur, correspondant au problème de décision suivant :

exemplaire : un groupe G_q d'ordre premier q pour lequel le problème du logarithme discret est réputé difficile, k générateurs distincts $g_1, \ldots, g_k$ de G_q, k éléments $a_1, \ldots, a_k \in \mathbb{Z}_q$, k éléments $b_1, \ldots b_k$ et deux éléments $A, B \in G_q$.

Problème : $A \stackrel{?}{=} \prod_{i=1}^{k} g_i^{a_i}$ et $B \stackrel{?}{=} \prod_{i=1}^{k} g_i^{b_i}$.

Ce protocole constitue une part essentielle du procédé de Brands, exploré en détail à la section 5.2.

2.5 Fonctions de hachage

Les *fonctions de hachage* [12] forment une classe fondamentale de primitives cryptographiques, permettant d'associer efficacement une chaîne de bits de longueur fixe à une chaîne de bits de longueur arbitraire. Elles sont d'une grande utilité, notamment dans

12. *Hash functions*.

le contexte de la signature numérique, où elles évitent la tâche fastidieuse de signer de longs messages. Plus formellement,

Définition 2.5.1 Une fonction de hachage $H_\ell : \{0,1\}^* \to \{0,1\}^\ell$ est une fonction pourvue au minimum des deux propriétés suivantes :

1° *(Compression)* — à une entrée x de taille arbitraire finie, H associe une sortie $H(x)$ de taille ℓ.

2° *(Efficacité)* — à partir de H et de x, il est facile de calculer $H(x)$.

Pour être sécuritaires dans un contexte cryptographique, les fonctions de hachage doivent remplir certaines exigences supplémentaires : une fonction de hachage H_ℓ est dite *à sens unique* [13] si, pour tout $y \in \{0,1\}^\ell$, il est difficile de déterminer une préimage x telle que $H(x) = y$; une fonction de hachage *cryptographique forte* [14] est une fonction de hachage H pour laquelle il est difficile de déterminer deux préimages distinctes x et x' telles que $H(x) = H(x')$. Nous utiliserons la notation $H(a_1, \ldots, a_k)$ pour signifier $H(a_1 \mid\mid \ldots \mid\mid a_k)$, où $a \mid\mid b$ dénote la concaténation des chaînes de bits a et b.

2.6 Cryptosystèmes

On nomme *cryptosystème* un procédé cryptographique offrant un service de communication confidentielle à deux entités — Alice et Bob par exemple ; ceux-ci doivent au préalable s'entendre — à l'abri des oreilles indiscrètes ! — sur une paire (e, d) de clés complémentaires. Pour envoyer un message m à Bob, Alice le *chiffre* à l'aide d'une transformation $E_e(m)$, obtenant ainsi le message chiffré c, qu'elle transmet à Bob ; celui-ci *déchiffre* alors c en appliquant la transformation $D_d(c)$ — l'inverse, en quelque sorte, de la transformation E_e — récupérant ainsi le message m en clair. Il doit être difficile de déterminer m si l'on ne dispose que du texte chiffré c, sans avoir accès aux clés (e, d). De façon plus formelle,

Définition 2.6.1 Soit un ensemble fini de textes en clair $\mathcal{M}$, un ensemble fini de textes chiffrés $\mathcal{C}$ et un ensemble fini de clés $\mathcal{K}$. Un cryptosystème est un ensemble de transformations $\{E_e : e \in \mathcal{K}\}$ et $\{D_d : d \in \mathcal{K}\}$ telles que, pour chaque paire de transformations complémentaires $E_e : \mathcal{M} \to \mathcal{C}$ et $D_d : \mathcal{C} \to \mathcal{M}$, et pour chaque $m \in \mathcal{M}$,

$$D_d(E_e(m)) = m.$$

Un cryptosystème doit également spécifier un algorithme (efficace) permettant la génération aléatoire de paires (e, d) de clés complémentaires.

13. *One-way*.
14. *Collision-resistant*.

Un principe fondamental [15] de la cryptologie moderne veut que la sécurité des cryptosystèmes ne dépende pas du secret des ensembles $\mathcal{M}, \mathcal{C}, \mathcal{K}, \{E_e : e \in \mathcal{K}\}$ et $\{D_d : d \in \mathcal{K}\}$, mais bien de celui des clés (e, d).

2.6.1 Cryptosystèmes à clé secrète

Le cryptosystème est dit *symétrique* ou *à clé secrète* [16] si, pour chaque paire de clés complémentaires d'encryption et de décryption (e, d), il est facile de déterminer d à partir de e et vice-versa. En pratique, pour la plupart des cryptosystèmes symétriques, $e = d$.

2.6.2 Cryptosystèmes à clé publique

Le cryptosystème est dit *asymétrique* ou *à clé publique* si, pour chaque paire de clés complémentaires d'encryption et de décryption (e, d), la *clé publique* e est disponible publiquement [17], alors que la *clé privée* d est gardée secrète. La sécurité du procédé dépend de la difficulté de déduire d, sachant e.

Un cryptosystème à clé publique est dit réversible si, pour tout $m \in \mathcal{M}$,

$$D_d(E_e(m)) = E_e(D_d(m)) = m.$$

2.6.3 Cryptosystème RSA

Une paire (e, d) de clés complémentaires RSA est une paire $((e, n), (d, n))$ où $n = p \cdot q$ satisfait aux exigences du problème de RSA (section 2.3.2), e est relativement premier à $\phi(n)$ et $d \equiv e^{-1} \pmod{\phi(n)}$. Pour $\mathcal{C} = \mathcal{M} = \mathbb{Z}_n$ et pour $x, y \in \mathbb{Z}_n$, on définit alors :

$$\begin{aligned} E_e(x) &= x^e \bmod n, \\ D_d(y) &= y^d \bmod n. \end{aligned}$$

Ce procédé fonde sa sécurité sur la difficulté présumée de résoudre le problème de RSA (section 2.3.2).

15. Il s'agit du principe de Kerckhoffs : « [...] *compromise of the system should not inconvenience the correspondents* [...] » (KAHN 1967), p. 235.

16. On réserve l'expression *clé secrète* aux cryptosystèmes symétriques et l'expression *clé privée* aux cryptosystèmes à clé publique.

17. Nous ferons l'hypothèse qu'il existe une infrastructure permettant la distribution sécuritaire de clés publiques dûment authentifiées.

2.7 Signature numérique

Les signatures numériques visent à émuler les fonctionnalités des signatures manuscrites dans le contexte dématérialisé des documents électroniques. Le signataire dispose d'un algorithme lui permettant d'apposer sa signature sur un document et rend disponible un algorithme de vérification complémentaire permettant à tout intéressé de vérifier l'authenticité de sa signature sur le document en question. De façon plus précise,

Définition 2.7.1 Soit un ensemble fini de messages $\mathcal{M}$, un ensemble fini de signatures $\mathcal{S}$ et un ensemble fini de clés $\mathcal{K}$; un procédé de signature numérique se compose d'un triplet $(\mathcal{M}, \mathcal{S}, \mathcal{K})$ tel que :

1° Pour toute clé $k \in \mathcal{K}$, il existe une fonction de signature sig_k et une fonction de vérification correspondante ver_k. La fonction sig_k est gardée secrète par le signataire alors que la fonction ver_k est publique.

2° Pour tout message $m \in \mathcal{M}$, toute clé $k \in \mathcal{K}$ et toute signature $\sigma \in \mathcal{S}$, les fonctions $sig_k : \mathcal{M} \to \mathcal{S}$ et $ver_k : \mathcal{M} \times \mathcal{S} \to \{vrai, faux\}$ vérifient

$$ver_k(m, \sigma) = vrai \Leftrightarrow \sigma = sig_k(m).$$

3° Pour tout message $m \in \mathcal{M}$ et toute clé $k \in \mathcal{K}$, il est difficile de déterminer un $\sigma \in \mathcal{S}$ tel que $ver_k(m, \sigma) = vrai$ si l'on ne dispose de ver_k, mais pas de sig_k, *i. e.* la contrefaçon de signatures est difficile.

Un cryptosystème à clé publique réversible se transforme aisément en un procédé de signature numérique. En effet, soit l'ensemble $\mathcal{M}$ des messages du procédé de signature, l'ensemble $\mathcal{C}$ des textes chiffrés du cryptosystème, l'ensemble $\mathcal{S}$ des signatures du procédé de signature, tels que $\mathcal{M} = \mathcal{C} = \mathcal{S}$. Soit (e, d) la paire de clés d'un cryptosystème à clé publique. On définit alors, pour tout message $m \in \mathcal{M}$ et toute signature $\sigma \in \mathcal{S}$,

$$\begin{aligned} sig(m) &= D_d(m), \\ ver(m, \sigma) &= vrai \Leftrightarrow E_e(\sigma) = m. \end{aligned}$$

En pratique, pour signer un message m de longueur arbitraire, on utilise une fonction de hachage cryptographique H_ℓ pour produire une *empreinte numérique*[18] z de taille fixe ℓ, calculée comme $z = H_\ell(m)$. La signature du procédé sur m est alors $\sigma = sig(z)$ et la fonction de vérification $ver(m, \sigma) = vrai \Leftrightarrow \sigma = sig(H_\ell(m))$. De façon à alléger la

18. *Message digest*.

description de protocoles déjà complexes, nous occulterons cette étape de la signature numérique.

2.7.1 Attaques sur les procédés de signature numérique

L'objectif d'un adversaire est de réussir à *contrefaire* des signatures, c'est-à-dire produire des paires (m, σ) telles que $ver(m, \sigma) = vrai$, où *ver* est la fonction de vérification associée à une certaine entité, autre que l'adversaire. On distingue généralement trois niveaux de bris d'un procédé de signature numérique : le *bris complet* est réalisé par un adversaire obtenant une fonction de signature fonctionnellement équivalente à celle du signataire ; la *contrefaçon sélective*, par un adversaire à même de créer une signature valide pour une certaine classe de messages déterminée a priori ; la *contrefaçon existentielle*, par un adversaire capable de contrefaire une signature pour au moins un message, mais avec peu (ou pas) de contrôle sur la forme du message.

2.7.2 Procédé de signature numérique RSA

Soit (e, n), une clé publique RSA, ainsi que (d, n), la clé privée correspondante. Pour tout message $m \in \mathcal{M}$ et pour toute signature $\sigma \in \mathcal{S}$, un procédé de signature numérique RSA a pour fonctions de signature et de vérification :

$$\begin{aligned} sig(m) &= m^d \bmod n, \\ ver(m, \sigma) &= vrai \Leftrightarrow \sigma \equiv m^e \pmod{n}. \end{aligned}$$

2.7.3 Procédé de signature numérique de Chaum-Pedersen

Ce procédé de signature est très apparenté aux signatures de Schnorr et, comme lui, base sa sécurité sur la difficulté du calcul de logarithmes discrets (section 2.3.3). Soit G_q, un groupe cyclique fini d'ordre q, et un générateur g de G, tels que le calcul de logarithmes discrets en base g y soit réputé difficile. La clé publique du procédé est formée du triplet (y, g, q) où y est un élément du groupe G_q et la clé privée correspondante consiste en un x tel que $y = g^x \bmod q$, c'est-à-dire que $x \equiv \log_g y \pmod{q}$.

Pour un message $m \in G_q$, la fonction de signature du procédé de Chaum-Pedersen consiste simplement en

$$sig(m) = m^x.$$

Pour une signature $z = sig(m)$, la fonction de vérification consiste en une preuve que

$$\log_g y = \log_m z,$$

i. e. le signataire démontre qu'il a bel et bien signé le message m à l'aide de sa clé privée x. Le signataire peut y arriver sans toutefois exhiber son secret x, en utilisant une preuve interactive comme celle illustrée à la figure 2.3 (les calculs étant effectués au sein du groupe G_q) :

$$
\begin{array}{lcr}
\mathcal{P}(m,g,x) & & \mathcal{V}(z,m,g,y) \\
\hline
w \in_{\mathcal{R}} \mathbb{Z}_q & & \\
a \leftarrow g^w & & \\
b \leftarrow m^w & & \\
 & \xrightarrow{a,b} & d \in_{\mathcal{R}} \mathbb{Z}_q \\
r = w + d \cdot x & \xleftarrow{d} & \\
 & \xrightarrow{r} & g^r = a \cdot y^d\,? \\
 & & m^r = b \cdot z^d\,? \\
\hline
 & & \textbf{oui/non}
\end{array}
$$

FIG. 2.3 - *Preuve interactive que* $\log_g y = \log_m z$

FIAT et SHAMIR (1987) ont montré comment transformer un tel protocole interactif en un procédé de signature non interactif en calculant le défi d comme $H(m,z,a,b)$, où H est une fonction de hachage cryptographique forte. Une signature de Chaum-Pedersen sur m devient alors un tuplet

$$\sigma = (z,a,b,r),$$

où, pour un w choisi aléatoirement au sein de $\mathbb{Z}_q$,

$$
\begin{aligned}
z &= m^x, \\
a &= g^w, \\
b &= m^w, \\
d &= H(m,z,a,b), \\
r &= w + d \cdot x.
\end{aligned}
$$

La procédure de vérification correspondante *ver*(m,σ) s'assure que, pour $d = H(m,z,a,b)$, les relations

$$
\begin{aligned}
g^r &= a \cdot y^d, \\
m^r &= b \cdot z^d
\end{aligned}
$$

soient vérifiées. Si H est une fonction de hachage cryptographique forte, alors le procédé de Chaum-Pedersen est sécuritaire en ce qui a trait à la contrefaçon existentielle de signatures, *i. e.* il est difficile pour une entité autre que le signataire de créer des paires (m, σ) telles que $ver(m, \sigma) = vrai$.

*   *   *

Ayant défini les blocs que nous assemblerons en de nombreux protocoles tout au long de ce mémoire, nous nous préoccupons à présent de définir précisément le concept de monnaie électronique, une tâche plus délicate qu'on pourrait le croire à premiere vue.

Chapitre 3

Fondements de la monnaie électronique

> « *À mesure que les transactions commerciales se multiplient, les sommes que l'on doit payer à la fois deviennent plus considérables, et le transport effectif des métaux précieux, d'un individu à un autre, présente ses inconvénients et ses difficultés.* »
> CHARLES BABBAGE, *Traité sur l'économie des machines et des manufactures.*

Une discussion portant sur une technologie aussi sophistiquée que la monnaie électronique se doit néanmoins de correctement définir une notion aussi triviale que celle de *monnaie*. Bien qu'il semble en exister autant de définitions que de manuels d'économique [1], nous dirons que la monnaie désigne *l'objet normalisé utilisé pour échanger des biens et des services*, de nos jours le papier-monnaie. Contrairement à la *monnaie-marchandise* — têtes de bétail, cigarettes, etc. — , le papier-monnaie est dépourvu de valeur intrinsèque : c'est ce qu'on appelle une *monnaie fiduciaire*, érigée comme moyen d'échange par force de décret gouvernemental. Le système monétaire moderne, basé sur la monnaie fiduciaire, repose sur la confiance globale des utilisateurs et sur les banques émettrices qui garantissent la monnaie — « ce billet a cours légal » — et s'appliquent à en restreindre la production. La monnaie remplit aussi un certain nombre de fonctions accessoires, qui ne lui sont pas exclusives : elle est par exemple l'unité normalisée servant à exprimer le coût des biens et des services et peut également jouer le rôle de réserve de valeur, c'est-à-dire un moyen de conserver la richesse dans le temps. [2] Notons

1. Selon DAVIES (1994), « *It is surprisingly difficult to establish a good definition of money* ». La nôtre est due à BAUMOL, BLINDER et SCARTH (1988).

2. Fonction cependant atténuée par l'inflation qui diminue avec le temps le pouvoir d'achat d'une monnaie.

qu'en divers lieux et à différentes époques, une quantité impressionnante d'objets les plus divers — du coquillage à la pièce d'or — ont rempli ces fonctions et que la monnaie fiduciaire, telle que nous la connaissons aujourd'hui, représente l'aboutissement d'une longue série d'expériences entreprises par le genre humain au fil des siècles et des civilisations pour tenter de résoudre le problème de l'échange efficace de biens et de services.

La définition moderne d'un *mécanisme de paiement* est qu'il a pour objet le transfert de fonds d'un individu à un autre [3] ; le plus simple de tous consiste en un simple échange de papier-monnaie. Si ce procédé est disponible à tous et «gratuit» — les coûts de production du papier-monnaie étant assumés par l'ensemble des contribuables — , il n'est cependant pas toujours pratique [4] ; les institutions financières offrent en conséquence d'autres mécanismes de paiement, le chèque par exemple. Contrairement aux banques centrales, qui gèrent la masse monétaire comme un bien collectif essentiel au bon fonctionnement de l'économie nationale, les institutions financières conçoivent et commercialisent ces mécanismes comme tout autre produit de consommation, dans le but d'en retirer un profit. Ces produits ne sont pas l'apanage des institutions financières : en fait, n'importe qui peut offrir un tel service s'il le désire, mais en général, seules les banques disposent de l'infrastructure financière et technologique, de même que de la crédibilité nécessaire à une telle entreprise.

Les *mécanismes de paiement électronique* sont caractérisés par l'échange d'informations électroniques transitant au travers de réseaux informatiques ou téléphoniques : on retrouve dans ce groupe les cartes de crédits, les cartes de guichet ainsi que les cartes de paiement prépayées. Les *procédés de monnaie électronique* forment un sous-ensemble de ce groupe, avec la caractéristique distinctive qu'ils visent à émuler certaines propriétés désirables du papier-monnaie — difficulté de la contrefaçon, *transférabilité* [5] , protection de la vie privée — tout en tirant profit des avantages du médium électronique — rapidité, facilité d'utilisation, sécurité fondée sur la cryptographie.

Si tous les mécanismes de paiement, électroniques ou non, offrent le même service fondamental de transfert de fonds, ils diffèrent cependant grandement dans leur façon d'atteindre cet objectif : ainsi, le papier-monnaie fonde sa sécurité sur la difficulté

3. Cette définition « fonctionnelle » est excessivement réductrice, niant entre autres la satisfaction des besoins psychologiques et sociaux associés au transfert de valeur. Ainsi, « *The tribes who, like the Ibo, stubbornly preferred cowries and manillas to coins, are eloquent examples of the persistence of their need for psychic satisfactions, in this case religious and ornamental gratification, to be combined with the more purely economic aspects of money, a combination lost by having to rely exclusively on the narrower range of functions performed by coins* » (DAVIES 1994). Un exemple bien contemporain est le prestige social associé à l'utilisation de certaines cartes de crédit.

4. De nos jours, il serait même suspect de payer votre nouvelle voiture en argent comptant, la loi exigeant que le fisc soit informé de tout paiement en espèces d'une valeur supérieure à 10 000$.

5. Intuitivement, ceci signifie que le papier-monnaie peut être échangé d'un individu à un autre sans intervention de la banque.

(relative) de le contrefaire, protège la vie privée des individus (bien que cela soit théoriquement possible, il est difficile de relier un billet quelconque à une transaction spécifique) et offre une grande souplesse d'utilisation. Les cartes de crédit, par contre, sont (relativement) faciles à contrefaire [6], ne protègent aucunement la vie privée des utilisateurs et ne peuvent être utilisées pour des transactions privées entre individus. Elles permettent cependant de s'acquitter facilement de gros montants, sont utilisables dans le monde entier et leur perte est souvent sans conséquence pour l'utilisateur. [7]

On voit que pour un même objectif — le transfert sécuritaire de valeurs — , plusieurs solutions très différentes peuvent exister. L'objectif de ce chapitre est d'énoncer un modèle abstrait propre à nous permettre de définir précisément et intelligiblement les propriétés et les fonctionnalités caractérisant les procédés de monnaie électronique.

La sécurité d'un procédé de monnaie électronique ne peut être uniquement tributaire de son ingéniosité cryptographique ; une multitude de facteurs peuvent faire échouer les objectifs de sécurité du procédé : réalisation fautive, gestion déficiente des clés, compromission de matériel prétendument « inviolable ». [8] Bien que la nomenclature de ces facteurs déborde de la nature essentiellement cryptographique de ce mémoire, nous soulignerons ceux qui ont un impact direct sur les fonctionnalités offertes par les procédés. [9]

3.1 Modèle

Pour décrire les procédés de monnaie électronique, nous utilisons la terminologie des systèmes distribués (BACON 1993). Un *système distribué* est un ensemble d'entités logiques capables d'interagir entre elles et avec l'*environnement* du système, au moyen d'un système de communication sous-jacent. [10] Une entité au sein de l'environnement est appelée un *usager*. Les usagers interagissent avec les entités internes au travers de *points d'accès* au système. Un *comportement d'interface* est une séquence d'entrées et de

6. Selon le chef de l'escouade chargée des fraudes par carte de crédit de Scotland Yard (NEWTON 1996), les faussaires offrent un produit d'aussi bonne qualité que les cartes authentiques et reproduisent les hologrammes depuis de nombreuses années.

7. Malgré l'insécurité de ce mécanisme de paiement, les utilisateurs fondent leur confiance sur le fait qu'ils seront remboursés en cas de vol et les institutions financières compensent pour les sommes perdues à la fraude par l'imposition de taux d'intérêt usuraires.

8. Pour ceux qui parfois se désespèrent du vaste fossé séparant théorie et pratique, le travail de Ross Anderson est particulièrement rafraîchissant à cet égard : il remarque (ANDERSON 1994 ; 1995) que les cryptosystèmes échouent généralement pour des raisons entièrement étrangères aux mathématiques et relate (ANDERSON et BEZUIDENHOUT 1995 ; 1996) la réalisation à grande échelle d'un procédé de paiement basé sur des techniques cryptologiques au sein d'une population rurale et économiquement défavorisée.

9. Nous avons été encouragé dans cette direction par PFITZMANN et WAIDNER (1996).

sorties aux points d'accès. Le *service* offert par un système distribué est l'ensemble de ses comportements d'interface possibles.

Un système distribué est défini par un certain nombre de spécifications :

1° La *spécification abstraite du service*, *i. e.* sa description, indépendamment de toute spécification interne du système.

2° La *spécification structurale du service*, *i. e.* la nomenclature des entités et la façon dont elles sont reliées les unes aux autres de même que la *description des protocoles* régissant leur réaction aux messages de l'environnement et des autres entités.

3° La *spécification des entités*, *i. e.* les règles de leur fonctionnement interne, de même que la description des *bidules* [11] les réalisant physiquement.

4° La *spécification concrète du service*, *i. e.* les détails syntaxiques de la représentation des comportements d'interface, tels que menus ou fenêtres, de même que les *règles d'utilisation* du système, c.-à-d. le mode d'emploi fourni au usagers.

Les descriptions cryptographiques de procédés n'incluent généralement que les spécifications abstraites et structurales ; ceci ne doit pas occulter le fait que la sécurité *globale* et l'utilité *pratique* d'un procédé dépend d'une interaction correcte de l'ensemble de ces éléments.

3.2 Entités

À chaque usager occupant un certain rôle dans l'environnement correspond un point d'accès et une entité interne au système. Les procédés de monnaie électronique définissent généralement les rôles suivants :

1° L'*acheteur*, souvent identifié à son *portefeuille*, et l'entité $\mathcal{U}$ correspondante. [12]

2° Le *marchand* et l'entité $\mathcal{S}$ correspondante.

3° La *banque* de l'acheteur et du marchand et l'entité $\mathcal{B}$ correspondante.

4° Le *juge* appelé à intervenir lors de disputes et son entité $\mathcal{J}$.

10. Il s'agit évidemment d'un canal de communication non sécuritaire, pour lequel un adversaire a la possibilité de *lire*, *éliminer*, *insérer* et *réordonner* l'information échangée.

11. *Devices*.

12. La définition de cette entité peut être raffinée : voir le chapitre 6.

L'entité $\mathcal{B}$ dissimule en son sein un ensemble complexe de banques et de réseaux financiers distincts, de mécanismes inter-bancaires de compensation et de virement des fonds, dont le détail ne nous préoccupera pas.

Certaines autres entités sont parfois définies : les *tiers fiables* $\mathcal{T}a$, de par la confiance générale dont ils jouissent, sont à même de simplifier un grand nombre de protocoles cryptographiques ; les *autorités de certification* $\mathcal{C}a$ ont pour tâche d'authentifier certaines informations, généralement les clés publiques des participants ; les fiduciaires $\mathcal{T}$ détiennent des informations sur les usagers qu'ils divulgueront lorsqu'un usager agira malhonnêtement. En général, nous ne ferons plus de distinction entre un usager, son rôle et l'entité interne correspondante.

3.3 Bidules

Les entités internes d'un procédé de paiement électronique sont généralement réalisées sous forme de bidules électroniques — portefeuille électronique pour les usagers, guichet automatique pour les banques — dont les aspects pertinents à notre propos sont :

1° Leur *puissance calculatoire* : pour les procédés de paiement, les bidules disposent d'une puissance calculatoire polynomiale. Ainsi, une carte munie d'une simple bande magnétique ne forme pas un bidule, mais plutôt un médium d'entreposage.

2° La *confiance* dont ils sont investis par les usagers : si la littérature regorge d'énoncés comme « un individu $\mathcal{A}$ fait confiance à un bidule $\mathcal{C}$ », un individu ne peut pourtant fonder cette confiance que par une évaluation systématique de l'ensemble des étapes du design, de la réalisation et de l'opération du bidule, tant du coté matériel que logiciel.[13] Comme le soulignent PFITZMANN et WAIDNER (1996) :

> « …*an important aspect of the usage of systems is that the trustworthiness of devices will and must be questioned in disputes, and this may be far more time-consuming than the digital dispute transactions.* »

3° Leur (présumée) *inviolabilité*[14] : il s'agit d'un aspect particulier de la confiance en un appareil, c'est-à-dire que $\mathcal{A}$ fait confiance au bidule $\mathcal{C}$, même lorsque ce

13. Cette question est étudiée plus en détail par PFITZMANN, PFITZMANN, SCHUNTER et WAIDNER (1996).
14. *Tamper-resistance.*

dernier se trouve entre les mains d'une entité $\mathcal{D}$. Cette inviolabilité est relative : il faut considérer probable qu'un adversaire déterminé, disposant de ressources adéquates, puisse en venir à bout. [15]

4° *Interaction sécuritaire* : les usagers *et* les bidules doivent disposer de dispositifs sécuritaires leur permettant de s'identifier mutuellement.

3.4 Fonctionnalités

Un procédé de monnaie électronique doit, avant tout, permettre de transférer des fonds de $\mathcal{U}$ à $\mathcal{S}$, à l'aide de protocoles appropriés. D'autres fonctionnalités, pertinentes à notre propos cryptographique, peuvent cependant grandement affecter son utilité pratique, par exemple, la *transférabilité*, la *divisibilité* et la *robustesse* [16].

3.4.1 Protocoles

Pour effectuer des transferts de fonds, un procédé de monnaie électronique doit être en mesure d'accomplir correctement les trois protocoles suivants :

1° un protocole de *retrait* entre $\mathcal{B}$ et $\mathcal{U}$ tel qu'à la conclusion du protocole, $\mathcal{U}$ dispose d'une pièce c et $\mathcal{B}$ aura débité du compte de $\mathcal{U}$ la valeur de la pièce c ;

2° un protocole d'*achat* entre $\mathcal{U}$ et $\mathcal{S}$ tel qu'au début du protocole, $\mathcal{U}$ dispose d'une pièce c et qu'à la conclusion du protocole, $\mathcal{S}$ dispose d'une pièce dépensée c' ; et

3° un protocole de *dépôt* entre $\mathcal{B}$ et $\mathcal{S}$ tel qu'au début du protocole, $\mathcal{S}$ dispose d'une pièce dépensée c' et qu'à la conclusion du protocole, $\mathcal{B}$ dispose d'une pièce déposée c'' et aura crédité au compte de $\mathcal{S}$ la valeur de c''.

Les procédés comportent parfois également un protocole de *création de compte* où l'identité de $\mathcal{U}$ par rapport à $\mathcal{B}$ est établie. Ces protocoles définissent un modèle triangulaire restreint d'interactions possibles entre $\mathcal{U}$, $\mathcal{S}$ et $\mathcal{B}$. C'est ce modèle qui sera sous-entendu pour l'ensemble des procédés présentés dans ce mémoire, sauf lorsque nous discuterons spécifiquement de la question de la transférabilité, au chapitre 8.

En pratique, il est également important de considérer l'efficacité relative de ces protocoles, c'est à dire le nombre d'interactions (*rounds*) entre les différentes entités et les

15. Pour une nomenclature des attaques sur les bidules dits inviolables, consulter ANDERSON et KUHN (1996). Voir aussi PFITZMANN, PFITZMANN, SCHUNTER et WAIDNER (1996) pour une catégorisation plus fine des bidules inviolables.

16. *Loss-tolerance*.

calculs requis de chaque entité pour leur exécution ; STADLER (1996) analyse en détail la complexité calculatoire de plusieurs des protocoles présentés dans ce mémoire.

3.4.2 Transférabilité et divisibilité

L'utilité pratique d'un procédé de monnaie électronique se trouve grandement accrue s'il est transférable, *i. e.* s'il est possible d'effectuer un paiement non seulement d'un individu à un marchand, mais également d'un individu à un autre individu. Le concept de transférabilité est étroitement associé à celui de divisibilité, c'est-à-dire la capacité de subdiviser une pièce d'une certaine valeur en d'autres de plus petite valeur. La combinaison de ces deux propriétés nous permet de régler des montants exacts de façon efficace, ce que nous explorerons en détail au chapitre 8.

Sauf indication contraire, nous ferons l'hypothèse que les procédés de monnaie électronique mentionnés dans ce mémoire offrent à cet égard une fonctionnalité réduite : le consommateur doit disposer de la monnaie exacte pour effectuer un paiement et effectuer autant de retraits de pièces de chaque dénomination qu'il lui est nécessaire.

3.4.3 Robustesse

Si la perte d'un portefeuille entraîne généralement la perte des devises qu'il contient, ce n'est pas nécessairement le cas pour d'autres procédés de paiement : la perte des cartes de crédit, si l'institution émettrice en est promptement avisée, entraîne rarement une pénalité. Un procédé de monnaie électronique pour lequel la perte du portefeuille n'entraîne pas une perte de valeur équivalente est dit *robuste*. Cette idée est explorée par WAIDNER et PFITZMANN (1990) et PFITZMANN et WAIDNER (1995).

3.5 Structure

Les principales caractéristiques structurales d'un mécanisme de paiement électronique sont la communication entre entités lors de l'exécution de protocoles — ce qui distingue les procédés *en lignes*[17] de ceux en *différé*[18] — et l'utilisation de matériel spécial.

Un procédé est dit en ligne s'il est nécessaire d'impliquer la banque lors de chaque exécution du protocole de paiement entre un consommateur et un marchand ; sinon, il

17. *Online*.
18. *Off-line*.

est dit en différé.[19] Si les procédés en ligne offrent en général de meilleures garanties de sécurité, ils imposent par contre une contrainte très restrictive dans le contexte de la monnaie électronique, celle de communiquer avec la banque lors de chaque exécution du protocole de paiement. Puisque ce sont les commerçants qui doivent faire les frais de cette communication, il est facile d'imaginer les problèmes d'engorgement que rencontrerait, par exemple, une bibliothèque facturant en temps réel, à des milliers d'utilisateurs, quelques sous par visionnement d'une image, d'un document ou d'une coupure de presse, forcée d'interagir avec une entité bancaire centrale pour vérifier chaque pièce ainsi dépensée. Pour ces raisons, ce mémoire se consacrera uniquement à l'étude des procédés en différé.

La plupart des systèmes proposés présupposent en pratique l'existence de certains types de matériel. Au minimum, ils requièrent la réalisation de points d'accès sécuritaires garantissant que chaque bidule ne puisse être utilisé que par son propriétaire légitime. Ils peuvent cependant exiger la réalisation de matériel spécialement conçu, comme pour les procédés de CHAUM et PEDERSEN (1992b) et de BRANDS (1994b) qui font l'objet du chapitre 6. Encore une fois, il s'agit de mesurer à quel point la sécurité du procédé dépend d'hypothèses faites sur les caractéristiques du matériel.

3.6 Sécurité

Un procédé de paiement doit identifier précisément les différents types d'attaques contre lesquelles il espère se prémunir. Il doit aussi déterminer les *hypothèses de fiabilité*[20] sous lesquelles cette sécurité est obtenue, c'est-à-dire qui fait confiance à qui. Il lui faut aussi identifier les conséquences d'interruptions subites des protocoles, qu'elles soient dues à des usagers malveillants ou à des défaillances du matériel (le réseau de communication sous-jacent, par exemple) : cette *résilience*[21] du procédé est d'une grande importance pratique.

3.6.1 Attaques

En général, nous considérerons que les participants à un système de paiement électronique sont à même de sécuriser leurs échanges, au moyen des procédés de chiffrement, d'authentification et de signature de leur choix. Cette question résolue, nous

19. Les cartes de crédit furent à l'origine conçues comme un système hybride, puisqu'il revenait au marchand d'obtenir une autorisation téléphonique pour les factures excédant une certaine limite ; le procédé est à présent entièrement en ligne.

20. *Trust model*.

21. *Fault tolerance*.

nous appliquerons à déterminer les différents comportements malhonnêtes possibles de la part des usagers, des commerçants, de même que de la banque [22], en utilisant uniquement l'information acquise au cours d'interactions avec d'autres participants ou encore par une mise en commun de cette information par une coalition de participants.

Attaques par un $\mathcal{U}$ malhonnête :

1° *Contrefaçon* : il est difficile à un $\mathcal{U}$ de créer une pièce c valide (c'est-à-dire acceptable à un $\mathcal{S}$) différente d'une des pièces qu'il a pu obtenir en exécutant un protocole de retrait avec $\mathcal{B}$.

2° *Réutilisation* [23] — version forte : supposons qu'un $\mathcal{U}$ ait obtenu une pièce c après avoir engagé un protocole de retrait avec $\mathcal{B}$; il lui est alors difficile de participer à deux protocoles d'achat avec un $\mathcal{S}_i$ et un $\mathcal{S}_j$ en utilisant chaque fois la même pièce c.

3° *Réutilisation* [24] — version faible : supposons qu'un $\mathcal{U}$ ait obtenu une pièce c après avoir engagé un protocole de retrait avec $\mathcal{B}$, qu'utilisant deux fois c, il participe à un protocole d'achat avec un $\mathcal{S}_1$, qui obtient ainsi une pièce c_1, et avec un $\mathcal{S}_2$, qui obtient ainsi une pièce c_2, et que ces deux pièces soient plus tard utilisées dans des protocoles de dépôt avec $\mathcal{B}$. Alors, de c_1 et c_2, l'on doit pouvoir déduire que la pièce c a été réutilisée, de même que l'identité de $\mathcal{U}$. [25]

Les procédés en différé ne permettent pas en général de se prémunir contre une attaque de type 2 (mais voir le chapitre 6) ; ils doivent alors se contenter d'une sécurité plus faible se limitant à la détection des attaques de type 3.

Attaques par un $\mathcal{B}$ malhonnête :

1° *Coup monté* par $\mathcal{B}$: supposons qu'un $\mathcal{B}$ malhonnête prétende qu'un $\mathcal{U}$ a réutilisé une pièce et présente à un juge $\mathcal{J}$ deux pièces déposées c_1 et c_2 ; alors ce dernier, muni des transcriptions des protocoles d'achat et de dépôt, conclura à la malhonnêteté de $\mathcal{B}$.

2° *Retrait frauduleux* : il est difficile à $\mathcal{B}$ de fournir une pièce invalide à un $\mathcal{U}$, suite à l'exécution d'un protocole de retrait entre $\mathcal{B}$ et $\mathcal{U}$.

---

22. S'il est en effet plausible de juger l'*institution* digne de confiance, il est cependant possible que des *employés* s'emparent de ses clés (cryptographiques) et les utilisent à mauvais escient.
23. *Strong integrity for the bank.*
24. *Weak integrity for the bank.*
25. Notons que si un escroc parvient à s'emparer d'un portefeuille et l'utilise pour des transactions frauduleuses, seuls le portefeuille et son propriétaire seront identifiés.

3º *Rejet frauduleux* d'un dépôt : supposons qu'un $\mathcal{U}$ et $\mathcal{B}$ participent ensemble à un protocole de retrait, que $\mathcal{U}$ et un $\mathcal{S}$ participent ensemble à un protocole d'achat, et que $\mathcal{S}$ et $\mathcal{B}$ participent ensemble à un protocole de dépôt. Alors, il est difficile à $\mathcal{B}$ de rejeter le dépôt de la pièce c sans qu'un juge $\mathcal{J}$, muni d'une transcription du protocole de dépôt, ne soit convaincu de sa malhonnêteté.

Attaques par un $\mathcal{S}$ malhonnête :

1º *Contrefaçon* : il est difficile à un $\mathcal{S}$ de créer une pièce c valide (c'est-à-dire acceptable à $\mathcal{B}$) différente d'une des pièces qu'il a pu obtenir en exécutant des protocoles d'achats avec des $\mathcal{U}_i$.

2º *Réutilisation* : supposons qu'un $\mathcal{S}$ participe à plusieurs protocoles de dépôt avec la même pièce c et que $\mathcal{B}$ obtienne ainsi deux pièces, c_1 et c_2. Alors, le fait que c a été réutilisée se déduit à partir de c_1 et c_2.

3º *Rejet frauduleux* d'un achat : supposons qu'un $\mathcal{U}$ et $\mathcal{B}$ participent ensemble à un protocole de retrait et que $\mathcal{U}$ et un $\mathcal{S}$ participent ensemble à un protocole d'achat utilisant la pièce c. Alors il est difficile à $\mathcal{S}$ de rejeter la pièce c sans qu'un juge $\mathcal{J}$, muni d'une transcription du protocole d'achat, ne soit convaincu de sa malhonnêteté.

D'autres types d'attaques sont parfois définies dans la littérature, mais leur exotisme les rend peu probables en pratique — par exemple, celles imaginées par JAKOBSSON et YUNG (1996).

3.6.2 Hypothèses de fiabilité

Chaque procédé doit spécifier les hypothèses de fiabilité en fonction desquelles la sécurité du procédé est assurée ; celles-ci établissent précisément le degré d'honnêteté attendu des entités, leur confiance mutuelle, la possibilité pour des participants de se liguer entre eux pour faire échouer les objectifs de sécurité, ainsi que la confiance accordée aux bidules par les participants. Évidemment, la sécurité de tout procédé cryptographique se doit de dépendre des hypothèses les plus faibles possibles quant au comportement de ses participants.

Pour la plupart des procédés, il sera implicite que les tiers fiables, tels qu'un juge $\mathcal{J}$ et les autorités de certification $\mathcal{C}a$, sont dignes de la confiance de tous les autres participants.

3.6.3 Résilience

Les transactions devraient idéalement être atomiques, mais ceci est impossible à assurer en pratique : les systèmes de communication sont faillibles et les participants, parfois malhonnêtes. On doit donc pouvoir garantir qu'aucun des participants n'obtienne un avantage indu et qu'aucun participant honnête ne subisse de perte, suite à l'interruption d'un protocole. Idéalement, les entités devraient être en mesure de détecter les interruptions et disposer de protocoles supplémentaires permettant la reprise de transactions interrompues. [26]

3.7 Vie privée

Un procédé de paiement protège la vie privée de ses usagers si aucune information les concernant (non pertinente à la transaction) n'est divulguée à des tierces parties. Les procédés électroniques présentent le potentiel de communiquer aux parties impliquées *plus* d'information qu'il n'est strictement nécessaire à la réalisation de la transaction : la protection de la vie privée est donc une fonctionnalité qui doit leur être explicitement ajoutée.

Cette protection est généralement offerte sous la forme de l'*anonymat de l'acheteur* et de la *non-corrélation de paiements*. Ces notions seront analysées en détail aux chapitres 4, 5 et 6. Récemment, le contexte politique tout particulier qui entoure les technologies cryptologiques a fait que l'on s'est intéressé à une forme plus restreinte de protection de la vie privée, l'anonymat *révocable*, qui fait l'objet du chapitre 7.

3.8 Armature

Nous présentons ici un procédé de paiement en différé utilisant un procédé de signature numérique avec fonctions de signature et de vérification *sig* et *ver*. Si le procédé de signature numérique utilisé est sécuritaire en ce qui a trait à la contrefaçon existentielle, alors il est difficile pour un utilisateur de contrefaire des pièces de monnaie. Le procédé est minimal, en ce qu'il n'offre aucune des caractéristiques — protection de la vie privée, divisibilité, etc. — discutées dans ce chapitre. Il formera en quelque sorte l'armature des procédés qui seront présentés tout au long de ce mémoire. Le protocole de retrait est illustré à la figure 3.1.

26. Bien que les questions reliées à la résilience soient presque systématiquement ignorées dans la littérature, PFITZMANN et WAIDNER (1996) soulignent que leur résolution a mobilisé une part importante des efforts des membres du projet CAFE (Boly *et al.*, 1994).

1° $\mathcal{U}$ envoie à $\mathcal{B}$ une demande de retrait.

2° $\mathcal{B}$ génère un numéro de série unique m et calcule $\sigma = sig(m)$.

3° $\mathcal{B}$ associe m à $\mathcal{U}$ dans son registre de retraits.

4° $\mathcal{B}$ transmet (m, σ) à $\mathcal{U}$ et débite son compte de v, la valeur de la pièce m.

FIG. 3.1 - *Procédé de base : protocole de retrait*

Le protocole d'achat, illustré à la figure 3.2, est valable pour des achats de valeur v exactement. Un scénario plus flexible suppose que la banque émet des pièces de différentes dénominations $\{v_i\}$. Elle dispose alors d'un ensemble de paires de fonctions de signature et de vérification $\{sig_i, ver_i\}$, une pour chaque dénomination. Sauf indication contraire (au chapitre 8 par exemple), c'est cet arrangement qui est sous-entendu pour tous les procédés de monnaie électronique présentés dans ce mémoire.

1° $\mathcal{U}$ présente (m, σ) à $\mathcal{S}$.

2° $\mathcal{S}$ vérifie que $ver(m, \sigma) = vrai$.

3° $\mathcal{S}$ remet les marchandises à $\mathcal{U}$.

FIG. 3.2 - *Procédé de base : protocole d'achat*

Le protocole de dépôt (figure 3.3) illustre bien que ce procédé ne peut empêcher un utilisateur malhonnête de réutiliser une même pièce deux fois, ce qui est typique des procédés en différé. Il permet par contre d'identifier l'usager en question puisque la banque est à même de retrouver le numéro de série m dans son registre de retraits, ce qui désignera $\mathcal{U}$ comme l'utilisateur ayant retiré m.

1° $\mathcal{S}$ présente (m, σ) à $\mathcal{B}$.

2° $\mathcal{B}$ vérifie que $ver(m, \sigma) = vrai$.

3° $\mathcal{B}$ vérifie dans sa base de données si m y est déjà inscrit. Le cas échéant, la pièce (m, σ) a été dépensée deux fois, sinon $\mathcal{B}$ y inscrit m.

4° $\mathcal{B}$ crédite le compte de $\mathcal{S}$ de v.

FIG. 3.3 - *Procédé de base : protocole de dépôt*

*　　*　　*

Si ce procédé brille par sa simplicité, ses nombreuses carences en font un candidat bien peu intéressant en tant que mécanisme de paiement. Les prochains chapitres seront consacrés à l'élaboration de procédés incorporant les différentes propriétés que nous avons identifiées comme désirables, c'est-à-dire protection de la vie privée, détection ou prévention de la réutilisation, divisibilité, etc.

Chapitre 4

Protection de la vie privée

> « *The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard.* [...] *You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.* »

La vision dépeinte par George Orwell (ORWELL 1949) d'un état policier où les technologies de télécommunication sont utilisées à des fins de contrôle et d'oppression de la liberté individuelle nous est désormais familière. [1] Bien peu de gens ignorent les dangers reliés à l'informatisation massive de l'infrastructure commerciale et de l'appareil bureaucratique, tant privé que public : l'acquisition par les organisations d'une quantité d'information toujours plus grande et toujours plus précise sur nos habitudes de vie, la concentration de cette information au sein de banques de données massives et les possibilités offertes par les recoupements entre ces banques de renseignements.

On serait ainsi porté à croire que chaque nouvelle économie, chaque nouveau gain d'efficacité dû à l'informatisation d'un nouveau champ de l'activité humaine est scrupuleusement examiné à la lumière de ses effets potentiellement pervers ; que le développement de technologies visant à remplacer des façons de faire millénaires — signature, papier-monnaie — est soigneusement évalué *avant* plutôt qu'*après* leur déploiement à grande échelle. [2]

1. MARX (1986) propose une discussion fascinante de la pertinence de cette vision pour la société informatisée d'aujourd'hui.
2. Justifiant ainsi les bien-nommées études *d'impacts sociaux* — généralement un morne constat des dommages au point d'impact.

En fait, du point de vue de la protection de la vie privée,[3] l'informatisation est un cauchemar : les solutions actuellement mises de l'avant exigent de l'utilisateur qu'il fonde sa confiance sur la bonne foi présumée des organisations,[4] sans pourtant lui fournir le moindre contrôle sur l'information qu'il divulgue ou génère au cours de transactions avec ces organisations. De leur coté, malgré les investissements importants nécessités par l'informatisation de leurs systèmes d'information, les organisations demeurent vulnérables à la fraude organisée.

C'est en réponse à cette problématique que David Chaum a publié, en 1985, un article qui devait faire époque dans le domaine de la cryptographie : « *Security Without Identification: Transaction Systems to Make Big Brother Obsolete* » (CHAUM 1985). Si d'emblée il annonçait ses couleurs — « *Computerization is robbing individuals of the ability to monitor and control the ways information about them is used* » —, il y définissait également une nouvelle approche où les organisations seraient à même de retirer les bénéfices espérés de l'informatisation et les utilisateurs, investis du pouvoir de protéger adéquatement leur vie privée.

Nous explorerons au cours de ce chapitre certaines des idées et des outils mis de l'avant par Chaum dans le contexte des procédés de monnaie électronique.

4.1 Réseaux anonymes

Une première approche au problème de la protection de la vie privée suppose que les transactions s'effectuent au sein d'un réseau offrant des communications anonymes non retraçables. Un tel réseau garantit aux utilisateurs que personne, ni même l'administrateur du réseau, n'est en mesure de déterminer l'émetteur et le destinataire d'un message y transitant.

---

3. La notion de vie privée (*privacy*) est étonnamment difficile à cerner ; le lecteur intéressé consultera avec bonheur ALDERMAN et KENNEDY (1995) pour un exposé anecdotique de ses principales problématiques, alors qu'une comparaison de sa conceptualisation au sein du droit français, américain, anglais et allemand est effectuée par RIGAUX (1990). COX (1994) offre un survol de l'application de cette notion au sein des différents procédés de monnaie électronique.

4. Même lorsqu'elles le sont, ce n'est pas toujours suffisant : considérez le cas du Gouvernement du Québec qui, en 1996, a accordé au ministère du Revenu des pouvoirs législatifs spéciaux lui permettant d'effectuer des recoupements entre plusieurs banques de données gouvernementales (Assurance-maladie, Régie de l'assurance-automobile) dans le but avoué d'un dépistage plus efficace des fraudeurs à l'impôt (le tout sans obtenir la permission des citoyens). Comme le souligne ANDERSON (1996) « [...] *the mere existence of such a potentially valuable resource will create strong political pressures for legitimized access by law enforcement agencies, insurance companies and others.* » Le cas du ficher national français SAFARI est encore plus frappant : créé en temps de guerre pour répondre à des exigences militaires, son existence relève d'une « *action spontanée et secrète de l'administration qui ne repose sur aucune base juridique solide* » (VITALIS 1988).

Un tel réseau ne peut être réalisé par la simple encryption du contenu du message. En effet, il est toujours possible à un observateur d'effectuer une *analyse du trafic* sur le réseau et en déduire ainsi entre qui, et à quel moment, s'effectuent les communications ; il est plutôt nécessaire soit de dissimuler l'identité de l'émetteur et du récipiendaire — ce qui est difficile —, soit de dissimuler leur relation, *i. e.* si l'on peut encore déterminer l'envoi ou la réception de messages, il est cependant impossible de relier le message issu de l'émetteur à celui reçu par le destinataire *(non-corrélation)*.

Une solution au problème de la non-corrélation de l'émetteur et du destinataire est proposée par CHAUM (1981) : un certain nombre de stations au sein du réseau — les *MIXs* — brouillent le trafic en recueillant, réordonnant et retransmettant (avec des délais variables) les messages en transit. En faisant circuler chaque message par une chaîne de MIXs, on s'assure qu'aucune analyse de trafic ne puisse efficacement corréler expéditeurs et destinataires — en autant qu'aucun individu ne contrôle l'ensemble des MIXs. [5]

Il est possible de *recevoir* anonymement un message sur un réseau, si chacun des utilisateurs du réseau le reçoit aussi — technique dite du *broadcast*. Il est possible d'*envoyer* anonymement un message par l'entremise d'un réseau du type décrit par CHAUM (1988). Ces techniques sont analysées en détail par PFITZMANN et WAIDNER (1986) : elles ont en commun d'introduire des désavantages importants en ce qui a trait à l'efficacité du réseau (délais de transmission, débit) ou d'exiger des hypothèses indésirables quant à l'honnêteté des acteurs impliqués. De plus, la disponibilité de tels réseaux est loin d'être assurée en pratique. Pour toutes ces raisons, une approche plus intéressante consiste à intégrer directement aux procédés de paiement les mécanismes de protection de la vie privée, plutôt que de dépendre de services offerts par le réseau de communication sous-jacent.

Dans ce contexte plus précis, deux saveurs principales de protection de la vie privée sont identifiées dans la littérature des procédés de monnaie électronique :

Définition 4.1.1 Un procédé de monnaie électronique protège l'*anonymat des paiements* [6] s'il est difficile pour $\mathcal{B}$ de relier une pièce déposée c à une instance particulière du protocole de retrait, même si $\mathcal{B}$ obtient la coopération de tous les $\mathcal{S}$.

Définition 4.1.2 Un procédé de monnaie électronique ne permet pas la *corrélation des paiements* [7] s'il est difficile pour $\mathcal{B}$ de déterminer si deux paiements distincts ont été ef-

5. Cette hypothèse n'est cependant pas nécessairement plausible dans le contexte de réseaux fermés comme les réseaux téléphoniques qui, dans plusieurs pays, sont contrôlés par une seule entité gouvernementale.

6. *Untraceable*.

7. *Unlinkable*.

fectués par le même $\mathcal{U}$, même en obtenant la collaboration de tous les $\mathcal{S}$.[8] Cette propriété implique nécessairement que l'anonymat des acheteurs est protégé lors des paiements.[9]

Il faut remarquer que si, à l'intérieur d'un procédé de monnaie électronique, la vie privée de l'individu peut être protégée, *i. e.* ni $\mathcal{S}$, ni $\mathcal{B}$ n'apprennent l'identité de $\mathcal{U}$ *à partir du paiement lui-même* et différents paiements ne peuvent être corrélés, rien n'empêche cependant qu'un utilisateur soit identifié — accidentellement ou délibérement — par *d'autres moyens*. En effet, les paiements effectués par l'entremise d'un réseau ne peuvent être davantage privés que les messages qui y transitent. Comme le soulignent PFITZMANN et WAIDNER (1996),

> « *Privacy of one system can never undo identification in the environment* [...]. *Addresses, timing, and amounts are information particularly likely to unintentionally undo the privacy of a payment system.* »

C'est dans ce contexte que nous étudions à présent les mécanismes de protection de la vie privée construits à même les procédés de monnaie électronique. C'est David Chaum qui a le premier décrit (CHAUM 1983; CHAUM 1984), puis réalisé (CHAUM 1985) un outil — la signature à l'aveugle — permettant la réalisation d'objectifs à prime abord irréconciliables : la sécurité sans l'identification.

4.2 Signatures à l'aveugle

Définition 4.2.1 Un procédé de *signature à l'aveugle*[10] est un protocole interactif impliquant deux entités, un vérificateur $\mathcal{A}$ et un signataire $\mathcal{E}$, tel qu'au début du protocole, $\mathcal{A}$ dispose d'un message m à faire signer par $\mathcal{E}$ et, à la conclusion du protocole, $\mathcal{A}$ dispose d'une signature σ sur le message m telle que $\mathcal{E}$ n'a vu ni σ, ni m.

Le protocole comporte trois phases : dans un premier temps, $\mathcal{A}$ camoufle le message m à l'aide d'un *masque* s choisi aléatoirement au sein d'un ensemble M de masques possibles et d'une fonction de masquage *blind*(s, m), produisant $\widetilde{m}$; $\mathcal{E}$ calculse ensuite la signature à l'aveugle $\widetilde{\sigma} = sig(\widetilde{m})$. Pour terminer, $\mathcal{A}$ récupère la signature σ sur m à l'aide d'une fonction de démasquage *unblind*$(s, \widetilde{\sigma})$.

8. Si un procédé protège l'anonymat des usagers mais permet la corrélation des transactions, alors il n'est toujours pas possible de relier un ensemble de paiements corrélés à un usager en particulier ; cependant, si un seul de ces paiements est identifié à un usager (peut-être par des moyens extérieurs au procédé, telle une simple identification visuelle), l'ensemble des paiements est alors relié à l'usager.

9. Ces caractéristiques ne sont évidemment valables que dans le contexte où un grand nombre de pièces sont en circulation.

10. *Blind signature scheme.*

Un tel procédé doit être *correct*, c'est-à-dire permettre au vérificateur d'obtenir une signature σ sur m telle que $ver(m, \sigma) = vrai$ et également lui assurer que la paire (m, σ) obtenue et la vue du signataire du protocole sont *statistiquement indépendantes* (*i. e.* non corrélées) et que le signataire est donc incapable de relier la paire (m, σ) à une exécution spécifique du protocole de signature.

Nous présentons deux réalisations distinctes de tels procédés : la première nous permettra d'illustrer simplement leur fonctionnement alors que la seconde forme le cœur des procédés de monnaie étudiés dans ce mémoire.

4.2.1 À la Chaum

Le procédé de signature RSA (section 2.7.2) forme la base du procédé de signature à l'aveugle proposé par CHAUM, FIAT et NAOR (1988), illustré à la figure 4.1. Il est fondé sur la propriété multiplicative du cryptosystème RSA, *i. e.* $(a \cdot b)^e \equiv a^e \cdot b^e \pmod{n}$.

Vérificateur$(m, (n, e))$		**Signataire**(n, d)
$s \in_{\mathcal{R}} \mathbb{Z}_n^*$		
$\widetilde{m} \leftarrow (s^e \cdot m) \bmod n$	$\xrightarrow{\widetilde{m}}$	
		$\widetilde{\sigma} \leftarrow \widetilde{m}^d \bmod n$
	$\xleftarrow{\widetilde{\sigma}}$	
$\sigma \leftarrow (s^{-1} \cdot \widetilde{\sigma}) \bmod n$		
(m, σ)		$(\widetilde{m}, \widetilde{\sigma})$

FIG. 4.1 - *Signature à l'aveugle à la Chaum*

Le vérificateur et le signataire disposent respectivement de la clé publique (e, n) et de la clé privée (d, n) d'un procédé de signature RSA. Le vérificateur choisit un masque s de façon aléatoire au sein du groupe $\mathbb{Z}_n^*$ et masque le message m à l'aide de la fonction *blind*$(s, m) = (s^e \cdot m) \bmod n$, obtenant ainsi $\widetilde{m}$. De son côté, le signataire signe cette valeur en utilisant la fonction de signature RSA *sig*$(\widetilde{m}) = \widetilde{m}^d \bmod n$, obtenant ainsi $\widetilde{\sigma}$. Le vérificateur récupère ensuite la signature (m, σ) à l'aide de la fonction *unblind*$(s, \widetilde{\sigma}) = (s^{-1} \cdot \widetilde{\sigma}) \bmod n$.

Le protocole est correct, puisque si le vérificateur et le signataire respectent le protocole, le vérificateur obtient une signature RSA (m, σ) sur le message m telle que

$$\sigma^e \equiv (s^{-1} \cdot \widetilde{\sigma})^e \equiv s^{-e} \cdot \widetilde{m} \equiv m \pmod{n}$$

et donc, $ver(m, \sigma) = vrai$. De plus, les paires (m, σ) et $(\widetilde{m}, \widetilde{\sigma})$ ne sont aucunement corrélées, puisque le masque s est un élément du groupe $\mathbb{Z}_n^*$ choisi aléatoirement. Ainsi, la vue du signataire du protocole et la paire (m, σ) sont statistiquement indépendantes.

4.2.2 À la Chaum-Pedersen

Le procédé de signature de Chaum-Pedersen (section 2.7.3) forme la base du procédé de signature à l'aveugle proposé par CHAUM et PEDERSEN (1992b). Comme précédemment, on y retrouve G_q, un groupe d'ordre q tel que le calcul des logarithmes discrets y est réputé difficile, un générateur g de G_q, la clé publique du procédé $y \in G_q$ ainsi que la clé privée correspondante x tel que $y = g^x \bmod q$, c'est-à-dire que $x \equiv \log_g y \pmod q$. On se souvient qu'une signature de Chaum-Pedersen sur un message $m \in G_q$ consiste en $z = m^x$ de même qu'une preuve que $\log_g y = \log_m z$.

Une signature *à l'aveugle* de Chaum-Pedersen est réalisée de façon similaire : le vérificateur commence par masquer le message m en choisissant un $s \in_{\mathcal{R}} \mathbb{Z}_q$ et calcule $A = blind(s, m) = m^s \bmod q$. Le signataire calcule alors $\tilde{z} = A^x \bmod q$ et le vérificateur peut récupérer la signature z sur m en calculant $unblind(s, \tilde{z}) = \tilde{z}^{(s^{-1})}$. Celui-ci nécessite également une preuve, non plus que $\log_g y = \log_m z$, mais plutôt que

$$\log_g y = \log_A \tilde{z}.$$

La preuve doit cependant être exécutée à l'aide de valeurs masquées, *i. e.* le signataire ne doit pas voir les a, b, d et r utilisés au cours de la preuve interactive, illustrée à la figure 4.2.

Dans un premier temps, le vérificateur masque le message m en un message A ; le signataire calcule alors $\tilde{z} = A^x$ ainsi que les valeurs a et b nécessaires à la preuve. Le vérificateur obtient z en démasquant A et effectue ensuite les calculs et les vérifications nécessaires à la preuve. Comme précédemment, la signature $\sigma = (z, a, b, r)$ sur m est correcte puisque, pour $d = H(m, z, a, b)$,

$$\begin{aligned} g^r &= a \cdot y^d, \\ m^r &= b \cdot z^d. \end{aligned}$$

Les paires (m, σ) et $(A, \widetilde{\sigma})$ sont statistiquement indépendantes puisqu'au cours du protocole, le signataire ne voit ni m, ni $\sigma = (z, a, b, r)$ mais bien plutôt A et $\widetilde{\sigma} = (\tilde{z}, \tilde{a}, \tilde{b}, \widetilde{r})$, et les masques appliqués à m, z, a, b et r sont tous des éléments aléatoires de $\mathbb{Z}_q$. Une preuve détaillée est offerte par CHAUM et PEDERSEN (1992b).

Vérificateur(m,g,y)		**Signataire**(g,x)
$s \in_{\mathcal{R}} \mathbb{Z}_q$, $t \leftarrow s^{-1}$ $A \leftarrow m^s$		
	$\xrightarrow{\quad A \quad}$	$\tilde{z} \leftarrow A^x$ $w \in_{\mathcal{R}} \mathbb{Z}_q$ $\tilde{a} \leftarrow g^w$ $\tilde{b} \leftarrow A^w$
$z \leftarrow \tilde{z}^t$ $u, v \in_{\mathcal{R}} \mathbb{Z}_q$ $a \leftarrow (\tilde{a} \cdot g^v)^u$ $b \leftarrow (\tilde{b}^t \cdot m^v)^u$ $d \leftarrow H(m, z, a, b)$ $\widetilde{d} \leftarrow d/u \bmod q$	$\xleftarrow{\quad \tilde{a}, \tilde{b}, \tilde{z} \quad}$	
	$\xrightarrow{\quad \tilde{d} \quad}$	$\widetilde{r} = w + \tilde{d} \cdot x$
$g^{\tilde{r}} = \tilde{a} \cdot y^{\tilde{d}}$? $A^{\tilde{r}} = \tilde{b} \cdot \tilde{z}^{\tilde{d}}$? $r \leftarrow (\widetilde{r} + v) \bmod q$	$\xleftarrow{\quad \widetilde{r} \quad}$	
(m, σ)		$(A, \widetilde{\sigma})$

FIG. 4.2 - *Signature à l'aveugle à la Chaum-Pedersen*

4.3 Un second procédé

Il nous est maintenant possible d'élaborer un second procédé de monnaie électronique, basé sur celui de la section 3.8, mais protégeant cette fois la vie privée de $\mathcal{U}$. On utilise à cet effet un procédé de signature à l'aveugle muni d'un ensemble de masques M et de fonctions de masquage et de démasquage *blind* et *unblind*. Les protocoles de retrait, d'achat et de dépôt sont illustrés aux figures 4.3, 4.4 et 4.5.

1° $\mathcal{U}$ génère un numéro de série unique m, un masque $s \in M$ et calcule $\widetilde{m} = \mathit{blind}(s, m)$.

2° $\mathcal{U}$ transmet $\widetilde{m}$ à $\mathcal{B}$.

3° $\mathcal{B}$ calcule $\widetilde{\sigma} = \mathit{sig}(\widetilde{m})$.

4° $\mathcal{B}$ transmet $\widetilde{\sigma}$ à $\mathcal{U}$ et débite son compte de v, la valeur de m.

5° $\mathcal{U}$ récupère la pièce (m, σ) en calculant $\sigma = \mathit{unblind}(s, \widetilde{\sigma})$.

FIG. 4.3 - *Procédé anonyme : protocole de retrait*

1° $\mathcal{U}$ transmet (m, σ) à $\mathcal{S}$.

2° $\mathcal{S}$ vérifie que $\mathit{ver}(m, \sigma) = \mathit{vrai}$.

3° $\mathcal{S}$ remet les marchandises à $\mathcal{U}$.

FIG. 4.4 - *Procédé anonyme : protocole d'achat*

1° $\mathcal{S}$ transmet (m, σ) à $\mathcal{B}$.

2° $\mathcal{B}$ vérifie que $\mathit{ver}(m, \sigma) = \mathit{vrai}$.

3° $\mathcal{B}$ vérifie dans sa base de données si m y est déjà inscrit. Le cas échéant, la pièce (m, σ) a été dépensée deux fois, sinon $\mathcal{B}$ y inscrit m.

4° $\mathcal{B}$ crédite le compte de $\mathcal{S}$ de v.

FIG. 4.5 - *Procédé anonyme : protocole de dépôt*

On voit que ce procédé est en tous points identique à celui présenté à la section 3.8, si ce n'est de l'utilisation d'un mécanisme de signature à l'aveugle. Ceci a cependant pour effet d'introduire un vice important : si l'anonymat de $\mathcal{U}$ est à présent adéquatement protégé, il lui est maintenant possible de réutiliser autant de fois qu'il le désire la pièce (m, σ). En effet, bien que $\mathcal{B}$ puisse déterminer si une pièce a été dépensée deux fois, elle n'est plus en mesure de relier cette pièce à une instance spécifique du protocole de retrait et d'identifier ainsi l'usager malhonnête. La vie privée de $\mathcal{U}$ ne semble pouvoir être protégée qu'en sacrifiant la sécurité de $\mathcal{B}$.

Une solution simple à ce dilemme consiste à permettre à $\mathcal{B}$ de vérifier la validité des pièces au cours du protocole d'achat, avec pour résultat de transformer notre procédé *en différé* en un procédé *en ligne*, caractéristique que nous avons déjà identifiée comme indésirable. Il nous faut donc explorer d'autres solutions possibles au problème de la détection de la réutilisation.

Chapitre 5

La détection de la réutilisation

Nous avons vu que si l'utilisation d'un procédé de signature à l'aveugle nous permet à présent de réaliser nos objectifs quant à la protection de la vie privée des utilisateurs, celui-ci introduit un vice inacceptable puisqu'il permet à des utilisateurs malhonnêtes de réutiliser les mêmes pièces plusieurs fois.

Une première solution à ce dilemme consiste à imposer aux usagers l'utilisation d'un portefeuille électronique inviolable émis par la banque, portefeuille qui se charge d'interdire la copie et la réutilisation d'une pièce. Cette solution présente le double désavantage de faire reposer la sécurité du procédé sur une hypothèse indémontrable — l'inviolabilité du portefeuille électronique — et d'exiger la production de matériel spécial et coûteux. Est-il possible d'arriver au même résultat par la seule utilisation de techniques cryptographiques ? Manifestement, il devient alors impossible d'empêcher la réutilisation, puisque si l'usager contrôle entièrement son portefeuille,[1] rien ne lui interdit de copier une pièce et d'en dépenser une première copie pour ensuite replacer les divers registres et compteurs du portefeuille aux valeurs qu'ils affichaient antérieurement à la dépense.

Une issue à cette impasse est d'accepter un modèle de sécurité plus faible, dans lequel, si la banque ne peut se prémunir contre la réutilisation de pièces, elle soit cependant en mesure d'identifier l'usager malhonnête *après coup*. Une telle approche exige la résolution de deux importants défis techniques :

1° Encoder l'identité de $\mathcal{U}$ dans la pièce de façon à ce qu'elle soit *dissimulée* lorsque $\mathcal{B}$ ne dispose que d'une seule copie de la pièce et *révélée* lorsque $\mathcal{B}$ dispose de deux copies de la même pièce.

1. C'est le cas, par exemple, lorsqu'un portefeuille électronique est implanté sous forme de logiciel exécuté par l'ordinateur personnel de l'usager.

2º Assurer que $\mathcal{B}$ n'authentifie que des pièces satisfaisant au premier critère, ce qui n'est pas simple puisque, justement, $\mathcal{B}$ signe *à l'aveugle* et n'a pas accès à la structure interne de la pièce !

Ces deux problèmes sont particulièrement difficiles à résoudre.[2] Une solution au premier est présentée à la section 5.1. Le second connaît plusieurs solutions distinctes[3] : CHAUM, FIAT et NAOR (1988) et FRANKLIN et YUNG (1992) utilisent la technique dite du *couper-et-choisir*[4], qui assure $\mathcal{B}$, avec une forte probabilité, que $\mathcal{U}$ a correctement construit les pièces. Cette probabilité dépend malheureusement de la construction et la transmission d'un grand nombre de pièces candidates pour chaque pièce authentifiée par $\mathcal{B}$, réduisant d'autant l'efficacité du protocole de retrait.

Si FERGUSON (1994) a introduit la notion de *single-term coins* — pièces signées à l'aveugle par $\mathcal{B}$ encodant l'identité de $\mathcal{U}$, mais construites en une seule opération — la technique qu'il présente ne semble pas destinée à passer à l'histoire. BRANDS (1993) a résolu la question en basant son système sur un problème jusqu'alors peu étudié, le problème du calcul des représentations (section 2.3.4). Nous présentons cette méthode originale et étonnamment flexible à la section 5.2.

5.1 L'encodage de l'identité

On désire encoder une certaine information au sein des pièces de telle façon que la possession d'une seule pièce n'apprenne rien à $\mathcal{B}$ sur $\mathcal{U}$, mais que si $\mathcal{U}$ réutilise la même pièce une seconde fois, il soit alors possible de l'identifier. La technique proposée ici utilise le fait que la pente d'une droite dans le plan est entièrement déterminée par deux points distincts sur cette droite, mais demeure indéterminée si un seul point est connu. De façon plus détaillée, soit un groupe G d'ordre p tel que le calcul de logarithmes discrets y est réputé difficile ; soit également un générateur g de G, deux éléments $u_0, u_1 \in G$, la droite définie par

$$y = (u_0 \cdot x + u_1) \bmod p \tag{5.1}$$

2. Selon Stefan Brands (1993) : « *Being able to detect double-spending by encoding the identity in the electronic cash is probably the single most difficult problem to resolve in privacy-protecting off-line cash systems not relying on tamper-resistance, and is what accounts for much of the inefficiency and unspecified functions.* »

3. Voir aussi (ABE et FUJISAKI 1996) pour une technique d'horodatation des signatures à l'aveugle.

4. *Cut-and-choose* ; à l'origine, un brillant protocole utilisé par les enfants — enfin, certains enfants — lorsque confrontés à la tâche difficile du partage équitable d'un morceau de gâteau : alors qu'un des enfants déplace le couteau sur le gâteau, le second lui indique à quel endroit effectuer la coupure ; le choix du morceau revient par contre au premier.

et soit $c = g^{u_0} \bmod p$ et $d = g^{u_1} \bmod p$. Alors, tout point (x, y) sur la droite définie en 5.1 doit également satisfaire à la relation

$$g^y \equiv c^x \cdot d \pmod{p}. \tag{5.2}$$

À partir de c, d, g et p, il est facile de vérifier la relation 5.2 pour un point (x, y) quelconque. Suivant l'hypothèse de la difficulté du calcul de logarithmes discrets dans le groupe G, il faut cependant disposer de la pente u_0 et de l'ordonnée à l'origine u_1 pour générer un point (x, y) sur la droite définie en 5.1.

À partir de deux points distincts (x_0, y_0) et (x_1, y_1) sur la droite, il est facile de calculer u_0 (et u_1) par la formule

$$u_0 \equiv \frac{y_0 - y_1}{x_0 - x_1} \pmod{p}. \tag{5.3}$$

Le tour est joué si la pente u_0 correspond à l'identité de $\mathcal{U}$ au sein du système : chaque fois que $\mathcal{U}$ désire dépenser une pièce, il doit par la même occasion générer un point aléatoire sur la droite déterminée par les coefficients u_0 et u_1 encodés dans la pièce. $\mathcal{S}$ vérifie alors que le point est bel et bien sur la droite à l'aide de la relation 5.2. Si $\mathcal{U}$ utilise plus d'une fois la même pièce, il aura alors fourni deux points distincts à partir desquels $\mathcal{B}$ pourra déterminer u_1 et ainsi son identité.[5]

5.2 Signature à l'aveugle restrictive

Si on désire que $\mathcal{U}$ encode correctement son identité dans les pièces qu'il fait signer à $\mathcal{B}$, alors les procédés de signature à l'aveugle sont peut-être trop puissants, puisqu'ils permettent d'obtenir une signature à l'aveugle du signataire *quel que soit le message m* et *quel que soit le masque s* utilisé. Stefan Brands a proposé (BRANDS 1993) une technique de signature à l'aveugle *restrictive*, basée sur le problème du calcul des représentations (section 2.3.4), qui impose la forme du message authentifié par $\mathcal{B}$ et le type de masquage appliqué par $\mathcal{U}$. Bien qu'elle puisse sembler plus complexe, cette technique se révélera beaucoup plus puissante et surtout très souple.

Cette technique est une variation de la signature à l'aveugle de Chaum-Pedersen (section 4.2.2), et les paramètres initiaux en sont identiques : un groupe fini cyclique $\mathbb{Z}_q$ d'ordre q, pour lequel le calcul d'une représentation est réputé difficile, des générateurs g, g_1 et g_2 de $\mathbb{Z}_q$ déterminés et rendus publics par $\mathcal{B}$, la clé privée $x \in_{\mathcal{R}} \mathbb{Z}_q$ de $\mathcal{B}$ de même

5. Plusieurs techniques similaires (qualifiées de *disposable authentication*) sont proposées par OKAMOTO et OHTA (1990).

que sa clé publique y telle que $y = g^x$. Certaines quantités sont ensuite déterminées lors de l'ouverture du compte de $\mathcal{U}$ chez $\mathcal{B}$.

5.2.1 Ouverture d'un compte

$\mathcal{U}$ choisit un nombre $u_1 \in_{\mathcal{R}} \mathbb{Z}_q$ qu'il garde secret et établit son identité avec $\mathcal{B}$ en calculant $I = g_1^{u_1}$. $\mathcal{B}$ conserve I avec l'identité réelle de $\mathcal{U}$ dans son registre des comptes. Dans ce procédé, dépenser deux fois la même pièce révèle nécessairement u_1, ce qui permet à $\mathcal{B}$ de calculer I et de déterminer l'identité de $\mathcal{U}$.

La quantité $m = I \cdot g_2$ joue un rôle fondamental dans ce système, puisqu'elle forme la structure interne de chaque pièce authentifiée par $\mathcal{B}$. Ce message est fixé une fois pour toutes à l'ouverture du compte — c'est le masque qui varie d'un retrait à un autre — et $\mathcal{B}$ peut ainsi déjà calculer sa signature $z = (I \cdot g_2)^x = (g_1^{u_1} \cdot g_2)^x$. Les étapes nécessaires à l'ouverture d'un compte sont illustrées à la figure 5.1.

1° $\mathcal{U}$ choisit son secret $u_1 \in_{\mathcal{R}} \mathbb{Z}_q$ et calcule son identité $I = g_1^{u_1}$, qu'il transmet à $\mathcal{B}$.

2° $\mathcal{B}$ conserve I avec l'identité officielle de $\mathcal{U}$. Il s'agit de son numéro de compte, qui doit être unique.

3° $\mathcal{B}$ calcule sa signature $z = m^x$ sur m et la transmet à $\mathcal{U}$.

FIG. 5.1 - *Procédé de Brands : ouverture de compte*

5.2.2 Protocole de retrait

Le procédé de Brands origine de la réalisation qu'il est suffisant de masquer différemment le *même* message m à chaque exécution du protocole de retrait pour obtenir l'indépendance statistique entre m et sa version masquée A. L'encodage de l'identité de $\mathcal{U}$ au sein du message m est tel qu'il n'est pas perturbé par l'opération de masquage. De façon plus formelle, Brands définit un protocole de signature à l'aveugle restrictif comme suit :

Définition 5.2.1 Soit le message $m \in G_q$ tel qu'au début du protocole de signature à l'aveugle, $\mathcal{U}$ connaît une représentation $(a_1, \ldots, a_k)$ de m par rapport aux générateurs $(g_1, \ldots, g_k)$. Soit un masque s, $A = \mathit{blind}(s, m)$ et la représentation $(b_1, \ldots, b_k)$ que $\mathcal{U}$ connaît de A à la fin du protocole. S'il existe deux fonctions I_1 et I_2 telles que

$$I_1(a_1, \ldots, a_k) = I_2(b_1, \ldots, b_2),$$

quels que soient le message m et le masque s, alors le protocole est un protocole de signature à l'aveugle *restrictif*.

Le protocole restrictif proposé par BRANDS (1993) définit $m = I \cdot g_2 = g_1^{u_1} \cdot g_2$ et sa version masquée comme $A = \mathit{blind}(m, s) = m^s = (g^{u_1 s} \cdot g_2^s)$ pour un masque $s \in_{\mathcal{R}} \mathbb{Z}_q$. Au début du protocole de signature, $\mathcal{U}$ connaît la représentation $(u_1, 1)$ de m par rapport à (g_1, g_2). À la fin du protocole, $\mathcal{U}$ connaît la représentation $(u_1 s, s)$ de A par rapport à (g_1, g_2). Ainsi, il existe des fonctions $I_1 = I_2$ telles que

$$I_1(a_1, a_2) = I_2(a_1, a_2) = a_1 / a_2 \bmod q,$$

puisque $I_1(u_1, 1) = I_2(u_1 s, s) = u_1$ et ce, quel que soit le masque s.

Pour effectuer un retrait, $\mathcal{U}$ présente son identité I à $\mathcal{B}$ et lui démontre qu'il possède une représentation de m par rapport aux générateurs (g_1, g_2), à l'aide de la technique du protocole de la section 2.4.1. Cette étape est importante, puisque $\mathcal{B}$ émet des pièces spécifiques à $\mathcal{U}$. L'usager et la banque exécutent ensuite le protocole de retrait de la figure 5.2 (nous nous contentons d'indiquer les lignes qui diffèrent du protocole de la figure 4.2).

$$\begin{array}{lcr}
\mathcal{U}(m) & & \mathcal{B}(m) \\
\hline
 & & \vdots \\
s \in_{\mathcal{R}} \mathbb{Z}_q & & \\
A \leftarrow m^s & & \tilde{b} \leftarrow m^w \\
\vdots & \vdots & \vdots \\
x_1, x_2 \in_{\mathcal{R}} \mathbb{Z}_q & & \\
B = g_1^{x_1} \cdot g_2^{x_2} & & \\
d \leftarrow H(A, B, z, a, b) & & \\
\vdots & \vdots & \vdots \\
\hline
(A, B, \sigma) & & (m, \tilde{\sigma})
\end{array}$$

FIG. 5.2 - *Procédé de Brands : protocole de retrait*

Ce protocole de retrait est basé sur le procédé de signature à l'aveugle de Chaum-Pedersen (section 4.2.2), dont nous rappelons brièvement le principe : pour obtenir une signature sur un message m, le vérificateur commence par choisir $s \in_{\mathcal{R}} \mathbb{Z}_q$ et masque m en calculant $A = \mathit{blind}(m, s) = m^s$. Il obtient $\tilde{z} = A^x$ de la part du signataire, de même qu'une preuve que $\log_g y = \log_A \tilde{z}$, exécutée avec des messages masqués. À la fin du protocole, le vérificateur possède une signature σ sur m, alors que le signataire n'a vu que $\tilde{\sigma}$ et A.

Dans le procédé de Brands, les rôles sont en quelque sorte inversés : le signataire a pleine connaissance du message m — c'est toujours le même pour un $\mathcal{U}$ donné —, mais ne verra jamais A. Le vérificateur obtient $z = m^x$ et une preuve que $\log_g y = \log_m z$. À la fin du protocole, le vérificateur possède une signature σ sur A, alors que le signataire n'a vu que $\widetilde{\sigma}$ et m.

Dans le but d'obtenir un protocole de paiement plus efficace, $\mathcal{U}$ choisit de plus x_1, $x_2 \in_{\mathcal{R}} \mathbb{Z}_q$ et calcule $B = g_1^{x_1} \cdot g_2^{x_2}$. Il obtient une signature sur B en calculant le défi comme $d = H(A, B, z, a, b)$. Comme précédemment, $\sigma = (z, a, b, r)$ et cette signature sur (A, B) est correcte si, pour $d = H(A, B, z, a, b)$,

$$\begin{aligned} g^r &= a \cdot y^d, \\ A^r &= b \cdot z^d. \end{aligned}$$

À la fin du protocole, $\mathcal{U}$ a en sa possession un triplet (A, B, σ) tel que $ver(A, B, \sigma) = vrai$ et il connaît les représentations $(u_1 s, s)$ de A et (x_1, x_2) de B par rapport à (g_1, g_2). Dans le procédé de Brands, ces trois conditions sont nécessaires pour pouvoir dépenser une pièce (A, B, σ).

5.2.3 Protocole d'achat et de dépôt

Pour effectuer un achat, $\mathcal{U}$ et $\mathcal{S}$ exécutent ensemble le protocole de la figure 5.3 : $\mathcal{U}$ exhibe une paire (A, B) de même qu'une signature σ sur (A, B). Il démontre aussi qu'il connaît une représentation de A et B par rapport aux générateurs (g_1, g_2), en utilisant la preuve interactive de la figure 2.2. Pour effectuer un dépôt, $\mathcal{S}$ transmet $(A, B, \sigma, d, r_1, r_2)$ à $\mathcal{B}$, qui effectue les mêmes vérifications.

$\mathcal{U}(A, B, \sigma)$		$\mathcal{S}$
	$\xrightarrow{A, B, \sigma}$	$ver(A, B, \sigma)$ = **vrai** ? $d \in_{\mathcal{R}} \mathbb{Z}_q$
$r_1 \leftarrow d(u_1 \cdot s) + x_1 \bmod q$ $r_2 \leftarrow ds + x_2 \bmod q$	$\xleftarrow{d}$	
	$\xrightarrow{r_1, r_2}$	$g_1^{r_1} \cdot g_2^{r_2} = A^d \cdot B$?
		$(A, B, \sigma, d, r_1, r_2)$

FIG. 5.3 - *Procédé de Brands : protocole d'achat*

Si $\mathcal{U}$ utilise deux fois la même pièce, cette irrégularité sera immédiatement repérable dans le registre de dépôts de $\mathcal{B}$, puisque le triplet (A, B, σ) sera identique pour deux exécutions distinctes du protocole de paiement. $\mathcal{B}$ disposera alors de paires de points (r_1, r_2) et (r_1', r_2') à partir desquels elle pourra déterminer — à l'aide de l'équation 5.3 — le secret u_1 de $\mathcal{U}$ comme étant

$$\frac{(r_1 - r_1')}{(r_2 - r_2')} \bmod q.$$

$\mathcal{B}$ peut ainsi calculer l'identité $I = g_1^{u_1}$ de $\mathcal{U}$ et rechercher cette quantité dans son registre de comptes.

Une caractéristique remarquable du procédé de Brands est que les communications entre $\mathcal{U}$ et $\mathcal{B}$ de même que celles entre $\mathcal{U}$ et $\mathcal{S}$ ne révèlent rien à un adversaire qui les épie. La création d'une pièce authentique à partir d'informations recueillies de la sorte lui impose de pouvoir calculer des logarithmes discrets au sein du groupe G_q. En théorie, les communications entre les différentes entités ne nécessitent donc aucun chiffrement supplémentaire.

*   *   *

Si les méthodes conjuguées des sections 5.1 et 5.2 permettent dorénavant l'identification d'un usager malhonnête, la simple détection du crime *après* qu'il ait été commis demeure une perspective peu attrayante pour les institutions bancaires : il serait nettement plus intéressant de pouvoir *prévenir* les comportements frauduleux. Bien que ceci implique l'utilisation de matériel spécial, nous explorons à présent des modèles où sont assouvis tant les exigences de sécurité des institutions financières que les besoins de confidentialité des utilisateurs.

Chapitre 6

Portefeuilles avec observateurs

La monnaie électronique et les problématiques qui lui sont associées ne représentent en fait qu'un cas particulier d'une situation beaucoup plus générale : en effet, pour fonctionner en société, les individus doivent obtenir d'organisations diverses des *créances*[1] de toutes sortes — certificat de naissance, permis de conduire, diplômes universitaires, preuves de crédit, etc. — qu'ils doivent ensuite présenter à d'autres organisations — forces de l'ordre, institutions d'enseignement, employeurs, commerçants — de façon à s'identifier et à leur démontrer qu'ils possèdent certaines qualifications. La monnaie électronique est une créance émise par les banques que les individus présentent aux commerçants, avec la particularité qu'elle ne peut l'être qu'une seule fois.[2]

Le cas général a été examiné à plusieurs reprises par David Chaum (CHAUM 1985; CHAUM et EVERTSE 1987; CHAUM et PEDERSEN 1992b). Il a remarqué que les exigences de sécurité des organisations consistent essentiellement à s'assurer que les créances qu'elles émettent ne puissent être modifiées ou contrefaites. Les individus, quant à eux, ont des besoins plus complexes :

1° s'assurer que les organisations ne puissent modifier d'autres créances que celles qu'elles émettent ;

2° s'assurer que les organisations ne puissent constituer des *dossiers* sur les individus, en mettant en commun les informations qu'elles détiennent à leur sujet ;

3° participer à certaines transactions de façon anonyme — paiement, études statistiques, etc.

Nous engageons quotidiennement de telles transactions avec une foule d'organisations, selon des règles et des procédures qui varient avec chacune. La plupart des sociétés

1. Credentials.
2. Ce qui justifie la terminologie de *one-show credential* que l'on retrouve parfois dans la littérature.

contemporaines, satisfaisant à la logique insatiable de rationalisation de l'appareil bureaucratique, contemplent actuellement le déploiement de technologies — principalement cryptologiques — visant à simplifier et uniformiser ces procédures.

Les systèmes envisagés à cet effet semblent privilégier l'un ou l'autre des participants, comme nous l'avons constaté au cours des trois chapitres précédents. Dans le premier cas, les individus sont à même de transiger avec les organisations sans devoir pour autant compromettre pour leur vie privée, mais le font au prix d'une sécurité affaiblie pour les organisations. Dans le second, les organisations jouissent d'une sécurité absolue, mais ne peuvent garantir à l'individu une protection adéquate de sa vie privée. Un des axes les plus importants du travail de Chaum porte sur la réconciliation de ces approches dans un modèle combinant les avantages de chacune. Ce chapitre est consacré à l'exploration d'un tel modèle dans le contexte de la monnaie électronique.

6.1 Dispositifs pour un portefeuille électronique

Jusqu'à présent, nous avons évité de préciser la nature du dispositif physique réalisant le procédé de monnaie électronique, si ce n'est des quelques caractéristiques que nous avons décrites à la section 3.3. En général, deux principaux types de dispositifs sont disponibles, qui correspondent précisément aux deux modèles que nous avons évoqués : ceux consistant en un ordinateur personnel et ceux à base d'un module inviolable.

6.1.1 Ordinateur

Un premier type de dispositif généralement proposé consiste en un ordinateur (ou autre engin calculatoire) exclusivement sous le contrôle des individus. En particulier, l'usager peut altérer toute section de la mémoire du bidule et contrôler l'ensemble de ses communications avec le monde extérieur.

Un tel système nous permet de réaliser efficacement un procédé de monnaie électronique offrant aux usagers une protection inconditionelle de la vie privée, à l'aide des techniques développées aux chapitres 4 et 5. Comme il a été précédemment mentionné, ce procédé est cependant tout à fait inefficace en ce qui à trait à la *prévention* de la réutilisation. En effet, il n'existe tout simplement aucun moyen purement cryptographique d'empêcher un utilisateur malhonnête de dépenser deux fois la même pièce de monnaie : au mieux est-il possible de le détecter et de l'identifier après coup. Ce type de système protège la vie privée des utilisateurs, mais ne peut offrir de garanties de sécurité solides aux organisations.

6.1.2 Module inviolable

Un second type de dispositif consiste en un module inviolable (une carte à puce, par exemple) émis par une organisation. Son utilisation permet d'obtenir aisément un système correct du point de vue des organisations puisque, pour le compromettre, un usager doit réussir à violer l'intégrité physique du module. Cependant, l'usager ne peut contrôler la nature des messages envoyés par le module : celui-ci pourrait fort bien communiquer aux organisations l'identité de l'usager et ainsi compromettre les caractéristiques d'anonymat attribuées au procédé. L'usager ne peut qu'espérer aveuglément que le système protège effectivement sa vie privée, sans pouvoir fonder cet espoir sur les caractéristiques du système.

6.1.3 Portefeuille électronique avec observateur

Puisque les deux scénarios mentionnés ci-haut ne permettent pas à eux seuls une solution satisfaisante, une solution hybride nous permettra peut-être d'obtenir les avantages de chacun. Une telle solution a été proposée par CHAUM et PEDERSEN (1992b) et subséquemment explorée par CRAMER et PEDERSEN (1994) et BRANDS (1994b).

Un *portefeuille avec observateur* consiste en un ordinateur, contrôlé par l'usager $\mathcal{U}$[3], et un module à accès protégé $\mathcal{O}$ — l'*observateur* — qui est en quelque sorte un intermédiaire agissant au nom de $\mathcal{B}$, et qui s'assure que $\mathcal{U}$ ne puisse dévier des protocoles prescrits par le système. De son coté, $\mathcal{U}$ est en mesure de communiquer librement avec le monde extérieur, mais $\mathcal{B}$ n'acceptera que les messages ayant été approuvés par $\mathcal{O}$. Celui-ci ne peut directement communiquer avec $\mathcal{B}$ mais peut refuser de coopérer avec $\mathcal{U}$, si ce dernier tente d'agir malhonnêtement. Le modèle distingue deux types de communication entre $\mathcal{B}$ et $\mathcal{O}$ qu'un procédé avec observateur doit considérer :

1° *Afflux*[4] : $\mathcal{B}$ ne peut communiquer à $\mathcal{O}$ aucune information supplémentaire, dans la mesure où $\mathcal{U}$ observe les protocoles, quel que soit le degré duquel $\mathcal{O}$ et $\mathcal{B}$ dévient des protocoles ;

2° *Fuites*[5] : $\mathcal{O}$ ne peut laisser transpirer aucune information supplémentaire à $\mathcal{B}$, dans la mesure où $\mathcal{U}$ observe les protocoles, quel que soit le degré duquel $\mathcal{O}$ et $\mathcal{B}$ dévient des protocoles.

Si les protocoles sont sécuritaires en ce qui a trait aux fuites, alors la sécurité en ce qui a trait à l'afflux n'est plus très significative, puisque $\mathcal{O}$ n'est plus en mesure de com-

3. Dans la discussion qui suit, nous ne ferons en fait aucune distinction entre un usager et son ordinateur.
4. *Inflow*.
5. *Outflow*.

muniquer à $\mathcal{B}$ l'information qu'il pourrait apprendre. Cependant, il faut considérer la situation où $\mathcal{O}$ est en mesure de conserver l'information transmise lors des protocoles et où $\mathcal{B}$ récupère $\mathcal{O}$ après une certaine période d'utilisation par $\mathcal{U}$. Dans un tel contexte, les protocoles se doivent d'être également sécuritaires par rapport à l'afflux. Lorsqu'un procédé est sécuritaire tant en ce qui à trait aux fuites qu'à l'afflux, on dit qu'il ne génère aucune *information commune*[6] à $\mathcal{O}$, $\mathcal{B}$ et $\mathcal{S}$.

6.2 Protocoles

Nous présentons une adaptation (BRANDS 1994b) du mécanisme de signature à l'aveugle restrictive (section 5.2) permettant la réalisation d'un portefeuille avec observateur ; les paramètres du système sont identiques à ceux de la section 5.2, c'est-à-dire que $\mathcal{B}$ rend disponible publiquement un triplet de générateurs (g, g_1, g_2) du groupe fini cyclique $\mathbb{Z}_q$, choisit sa clé secrète $x \in_{\mathcal{R}} \mathbb{Z}_q$ et publie sa clé publique y telle que $y = g^x$.

Lorsque $\mathcal{U}$ désire ouvrir un compte, $\mathcal{B}$ lui fournit un observateur contenant un secret o_1 en mémoire non volatile. $\mathcal{U}$ choisit un secret $u_1 \in_{\mathcal{R}} \mathbb{Z}_q$, calcule $g_1^{u_1}$ qu'il transmet à $\mathcal{B}$. Celle-ci calcule $A_{\mathcal{O}} = g_1^{o_1}$ et $I = (A_{\mathcal{O}} \cdot g_1^{u_1})$. Comme précédemment, $m = I \cdot g_2$ et $z = m^x$, quantités que $\mathcal{B}$ calcule et transmet à $\mathcal{U}$. Le processus est illustré à la figure 6.1.

1º $\mathcal{U}$ choisit son secret $u_1 \in_{\mathcal{R}} \mathbb{Z}_q$ et calcule $g_1^{u_1}$ qu'il transmet à $\mathcal{B}$.

2º $\mathcal{B}$ fournit à $\mathcal{U}$ un observateur $\mathcal{O}$ contenant en mémoire non volatile un nombre aléatoire $o_1 \in_{\mathcal{R}} \mathbb{Z}_q$.

3º $\mathcal{B}$ calcule $A_{\mathcal{O}} = g_1^{o_1}, I = (A_{\mathcal{O}} \cdot g_1^{u_1})$ ainsi que $z = (I \cdot g_2)^x = m^x$ et transmet $A_{\mathcal{O}}$ et z à $\mathcal{U}$, qui les conserve précieusement.

FIG. 6.1 - *Procédé avec observateur : ouverture d'un compte*

Dans ce système, I représente toujours le numéro de compte de $\mathcal{U}$; cependant, contrairement au procédé de base, $\mathcal{U}$ ne connaît pas $\log_{g_1} I$ et, par conséquent, ne connaît plus *à lui seul* une représentation de m par rapport à (g_1, g_2), tout comme $\mathcal{O}$. Ce n'est qu'ensemble qu'ils connaissent la représentation $(o_1 + u_1, 1)$ de m par rapport à (g_1, g_2). Ceci sera utilisé au cours du protocole de paiement, puisque $\mathcal{U}$ devra absolument obtenir la collaboration de $\mathcal{O}$ pour dépenser une pièce, à moins qu'il n'ait réussi à s'emparer de o_1 en violant l'intégrité physique de $\mathcal{O}$.

6. *Shared information*.

Pour empêcher $\mathcal{U}$ de réutiliser la même pièce, $\mathcal{O}$ va générer un secret o_2 pour chaque pièce obtenue au cours du protocole de retrait illustré à la figure 6.2. Le principe est le suivant : pour chaque pièce, $\mathcal{O}$ choisit un élément $o_2 \in_{\mathcal{R}} \mathbb{Z}_q$ qu'il conserve ensuite en mémoire (notée $\{o\}$). Cet élément fera partie de la représentation de la pièce que $\mathcal{B}$ signera subséquemment. Lorsque $\mathcal{U}$ voudra dépenser une pièce, il devra obtenir o_2 de $\mathcal{O}$ pour pouvoir démontrer à $\mathcal{S}$ qu'il possède une représentation de la pièce. Une fois que $\mathcal{O}$ aura fourni o_2 à $\mathcal{U}$, il l'effacera de sa mémoire, empêchant ainsi $\mathcal{U}$ de dépenser deux fois la pièce.

$\mathcal{O}(\{o\})$		$\mathcal{U}$		$\mathcal{B}$
$o_2 \in_{\mathcal{R}} \mathbb{Z}_q$				
$B_{\mathcal{O}} \leftarrow g_1^{o_2}$				
	$\xrightarrow{B_{\mathcal{O}}}$	$\vdots$	$\vdots$	$\vdots$
$\{o\} \leftarrow \{o\} \cup o_2$		$x_1, x_2, e \in_{\mathcal{R}} \mathbb{Z}_q$		
		$B = g_1^{x_1} \cdot g_2^{x_2} A_{\mathcal{O}}^{se} B_{\mathcal{O}}$		
		$\vdots$	$\vdots$	$\vdots$
$(o_1, \{o\})$		$(A, B, \sigma, A_{\mathcal{O}}, B_{\mathcal{O}}, e)$		$(m, \widetilde{\sigma})$

FIG. 6.2 - *Procédé avec observateur : protocole de retrait*

À la fin du protocole, $\mathcal{U}$ obtient un triplet (A, B, σ) tel que $ver(A, B, \sigma) = vrai$, mais, contrairement au procédé sans observateurs, $\mathcal{U}$ n'est pas en mesure, sans la collaboration de $\mathcal{O}$, de démontrer qu'il connaît des représentations de A et de B par rapport à (g_1, g_2), puisque la représentation de $A = (A_{\mathcal{O}} \cdot g_1^{u_1} \cdot g_2)^s$ est $((o_1 + u_1)s, s)$, et que la représentation de $B = g_1^{x_1} \cdot g_2^{x_2} A_{\mathcal{O}}^{se} B_{\mathcal{O}}$ est $(x_1 + o_1 se + o_2, x_2)$.

Le protocole de paiement est illustré à la figure 6.3. Pour pouvoir démontrer à $\mathcal{S}$ qu'il connait des représentations de A et de B, $\mathcal{U}$ doit obtenir de $\mathcal{O}$ une combinaison linéaire r_1' de o_1 et o_2. $\mathcal{O}$ vérifie tout d'abord si o_2 est en mémoire. Le cas échéant, $\mathcal{O}$ fournit r_1' à $\mathcal{U}$ et efface ensuite o_2 de sa mémoire ; sinon, $\mathcal{O}$ refuse tout simplement de collaborer, puisque cela indique que $\mathcal{U}$ tente de dépenser une pièce pour une seconde fois.

Si jamais $\mathcal{U}$ réussit à violer les protections de $\mathcal{O}$, il est alors en mesure de dépenser les pièces plus d'une fois ; cependant, tout comme dans le procédé de base, à partir de points (r_1, r_2) et (r_1', r_2') obtenus par deux exécutions du protocole de paiement, $\mathcal{B}$ est

$$
\begin{array}{lclcr}
\mathcal{O}(o_1, \{o\}) & & \mathcal{U}(A, B, \sigma, A_{\mathcal{O}}, B_{\mathcal{O}}, e) & & \mathcal{S} \\
\hline
 & & \vdots & & \vdots \\
o_2 \in \{o\}\,? & \xleftarrow{d'} & d' \leftarrow s \cdot (d + e) & \xleftarrow{d} & \\
r'_1 \leftarrow d' o_1 + o_2 & & & & \\
 & \xrightarrow{r'_1} & g_1^{r'_1} = A_{\mathcal{O}}^{d'} B_{\mathcal{O}}\,? & & \\
\{o\} \leftarrow \{o\}/o_2 & & r_1 \leftarrow r'_1 + d(u_1 s) + x_1 & & \\
 & & r_2 \leftarrow d \cdot s + x_2 & & \\
 & & & \xrightarrow{r_1, r_2} & \vdots \\
\hline
(o_1, \{o\}) & & & & (A, B, \sigma, r_1, r_2)
\end{array}
$$

FIG. 6.3 - *Procédé avec observateur : protocole d'achat*

toujours en mesure de calculer

$$u_1 = \frac{(r_1 - r'_1)}{(r_2 - r'_2)} - o_1,$$

et ainsi, de déterminer l'identité I de $\mathcal{U}$.

* * *

On pourrait croire que le modèle des portefeuilles avec observateur répresente le meilleur des mondes possibles, propre à satisfaire à la fois les individus et les organisations dans leur recherche de sécurité. Nous verrons dans un instant que ce n'est pas tout à fait exact et qu'il faut tenir compte d'une nécessité qui leur est « supérieure » — la *sécurité de l'État*.

Chapitre 7

Révocabilité

La protection de la vie privée nous est apparue jusqu'à présent comme une valeur fondamentalement positive, dont la pertinence ne semble plus à démontrer. Cet anonymat dont désirent légitimement se prévaloir les citoyens respectueux des lois peut cependant favoriser des abus frauduleux du système (par exemple, le blanchiment de l'argent par le crime organisé). Ce type d'abus est examiné avec beaucoup de sérieux par les autorités, comme le souligne un rapport du Congrès américain (OTA 1995) :

> « *The control of crime is central to the functions of modern governments, in the maintenance of a stable social order. The sovereignty of the state may be at stake, in its inability to control money across borders and protect the integrity of its currency. The state's decision regarding what to criminalize lies at the heart of sovereignty, a decision increasingly undermined by the impunity with which the money launderer moves money across international borders.* »

La dissimulation des avoirs monétaires — dont le blanchiment de l'argent n'est qu'une des formes possibles [1] — est un crime qui se renouvelle avec chaque nouveau mécanisme de transfert des avoirs offert par les institutions financières. Dans cette optique, les institutions financières ainsi que les forces de l'ordre sont soucieuses d'identifier et de prévenir les nouveaux types de fraude offerts par les procédés de monnaie électro-

1. Selon ce même rapport (OTA 1995), il y a plusieurs bonnes raisons pour désirer cacher ses états financiers aux autorités : la protection des avoirs personnels ou commerciaux menacés par des recours judiciaires (poursuites ou procédures de divorce par exemple) ; l'évasion fiscale, tant celle d'individus que de sociétés commerciales ; la fuite de capitaux d'un pays à une autre, à la suite de changements économiques, politiques ou sociaux ; le délit d'initié dans le domaine des valeurs boursières ; les activités gouvernementales secrètes, telles que le contre-espionnage; et enfin, la contrebande.

nique.[2] Ainsi, la très sérieuse *Banque des Règlements Internationaux* émet cette mise en garde (BIS 1996) :

> « *Some characteristics of certain electronic money products, such as their relative lack of physical bulk, their potential anonymity and the possibility of effecting fast, remote transfers, might make them more susceptible than traditional payment systems to criminal activities, in particular money laundering.* »

Un autre facteur propre à influencer cet aspect du développement des procédés de monnaie électronique est la nature très particulière des relations qui unissent les gouvernements et la science cryptologique[3] : de nombreux gouvernements demeurent inquiets de voir se disséminer librement des technologies qui, il y a quelques années à peine, relevaient du secret militaire le plus strict.[4]

Dans le but de réduire cette tension inhérente entre les besoins de confidentialité des usagers et ceux de contrôle des États et des forces de l'ordre, MICALI (1992) a introduit la notion de cryptosystème *équitable*[5] : un tel procédé offre encore à ses utilisateurs les services de confidentialité pour lesquels il a été originalement conçu, avec la caractéristique supplémentaire qu'il est possible de *révoquer* cette confidentialité lorsque la situation l'exige. Cette situation est généralement décrite comme celle où les autorités policières, après avoir obtenu les autorisations adéquates d'une cour de justice, désirent épier les conversations d'individus soupçonnés d'activités illégales.

Pour réaliser la révocabilité au sein d'un procédé cryptographique, une première approche suggère d'incorporer cette capacité à même le procédé sous forme de *brèche secrète* — un défaut de fabrication en quelque sorte, mais connu des seuls concepteurs du système. Une telle approche suppose que cette brèche puisse demeurer secrète, hypothèse dangereuse et peu réaliste : il est beaucoup plus sûr de confier la capacité de révocation à un tiers fiable, un *fiduciaire*[6], noté $\mathcal{T}$. La sécurité du système repose alors sur l'incorruptibilité du fiduciaire, hypothèse non démontrable, mais dont la crédibilité peut être renforcée à souhait en partageant la capacité de révocation parmi plusieurs fiduciaires.

2. VON SOLMS et NACCACHE (1992) imaginent comment un $\mathcal{U}$ malhonnête pourrait obtenir le paiement d'une rançon en monnaie électronique — un « million de dollars en petites coupures » numérique en quelque sorte — dans le contexte d'un procédé de monnaie anonyme en ligne semblable à celui de la section 4.3. JAKOBSSON (1995a) explore les nouvelles possibilités offertes aux maîtres-chanteurs par les signatures numériques dites « incontestables ».

3. Voir LANDAU (1983 ; 1988) pour le récit de quelques étapes « croustillantes » du développement de cette relation malaisée.

4. Pour un compte-rendu complet du « débat cryptographique » voir HOFFMAN (1995).

5. *Fair cryptosystem*.

6. *Trustee*.

Dans le contexte des procédés de monnaie électronique, la notion de révocabilité a reçu une attention considérable de la part de la communauté scientifique [7]. DAVIDA, FRANKEL, TSIOUNIS et YUNG (1997) ont énoncé les caractéristiques souhaitables de cette nouvelle fonctionnalité :

1° *Révocabilité* : si l'anonymat des acheteurs peut être révoqué, cela ne doit être possible que par l'entremise d'un fiduciaire $\mathcal{T}$;

2° *Séparation des pouvoirs* : le fiduciaire ne dispose d'aucun autre pouvoir que celui de révoquer l'anonymat de $\mathcal{U}$. En particulier, il ne peut s'adonner à la contrefaçon ou organiser un coup monté contre $\mathcal{U}$;

3° *Impotence* : même en obtenant la collaboration de $\mathcal{T}$, $\mathcal{B}$ n'est pas en mesure d'organiser avec succès un coup monté contre $\mathcal{U}$;

4° *Sélectivité* : la révocation doit être sélective, c'est-à-dire n'affecter que la seule transaction pour laquelle une cour a émis un mandat. Le système doit donc permettre de retracer complètement l'historique de cette transaction, mais préserver l'anonymat complet de toute autre transaction, en particulier toute autre transaction du $\mathcal{U}$ concerné ;

5° *Efficacité* : les protocoles permettant la révocabilité se doivent non seulement d'être efficaces, mais aussi d'imposer des délais minimaux au système, pour toutes les entités $\mathcal{B}$, $\mathcal{U}$ et $\mathcal{S}$. En particulier, $\mathcal{T}$ ne devrait être impliqué que dans les seules transactions où l'anonymat doit être révoqué.

La révocation de l'anonymat nécessite l'ajout de deux protocoles supplémentaires : un protocole d'*identification de l'utilisateur* [8], permettant d'exposer l'identité du propriétaire d'une certaine pièce, et un protocole d'*identification de pièce* [9], permettant de déterminer où a été dépensée une pièce spécifique. Dans le premier cas, $\mathcal{B}$ présente à $\mathcal{T}$ une transcription du protocole de dépôt et $\mathcal{T}$ lui fournit en retour une information par laquelle $\mathcal{B}$ peut identifier le propriétaire de la pièce, par le biais des renseignements qu'elle conserve sur ses clients. Ce protocole permet donc de retracer l'origine de pièces suspectes, par exemple celles déposées par un commerçant suspecté de blanchiment d'argent. Dans le second cas, $\mathcal{B}$ présente à $\mathcal{T}$ la transcription du protocole de retrait effectué par un individu suspect et $\mathcal{T}$ lui fournit l'information qui apparaîtra lorsque la pièce sera déposée chez $\mathcal{B}$. Le protocole appose en quelque sorte un numéro de série à

---

7. En témoignent les publications suivantes : CAMENISCH, PIVETEAU et STADLER (1994), BRICKELL, GEMMELL et KRAVITZ (1995), STADLER, PIVETEAU et CAMENISCH (1995), CAMENISCH, PIVETEAU et STADLER (1996), STADLER (1996), CAMENISCH, MAURER et STADLER (1996), JAKOBSSON et YUNG (1996), FRANKEL, TSIOUNIS et YUNG (1996) ainsi que DAVIDA, FRANKEL, TSIOUNIS et YUNG (1997).

8. *Owner-tracing* ou encore, *backward-traceability*.

9. *Coin-tracing* ou encore, *forward-traceability*.

la pièce, permettant ainsi de déterminer où un individu spécifique dépense sa monnaie électronique.

Pour satisfaire la caractéristique de *sélectivité*, un procédé révocable doit inclure les deux types de protocoles : en effet, si une pièce spécifique doit être retracée à travers le système et que seule l'identification de l'utilisateur est offerte, $\mathcal{T}$ est forcé de révoquer l'anonymat de *toutes* les pièces pour retrouver la pièce provenant d'un retrait spécifique. De même, si seule l'identification de pièce est offerte, déterminer le propriétaire d'une certaine pièce nécessite de révoquer l'anonymat de tous les retraits.

7.1 Protocoles pour un procédé révocable

Une fois de plus, notre point de départ sera le procédé de Brands (section 5.2) : la flexibilité du problème de calculer une représentation, sur lequel il est fondé, permet d'ajouter facilement une telle fonctionnalité sans devoir effectuer de modifications importantes aux protocoles qui nous sont désormais familiers. Les paramètres initiaux sont presque identiques : un groupe $\mathbb{Z}_q$ où le calcul du logarithme discret est réputé difficile ; des générateurs (g, g_1, g_2) et un générateur supplémentaire g_3 de $\mathbb{Z}_q$; la clé secrète $x \in_{\mathcal{R}} \mathbb{Z}_q$ de $\mathcal{B}$ ainsi que sa clé publique $y = g^x$. À la création du système, $\mathcal{T}$ établit sa présence en choisissant sa clé privée $x_{\mathcal{T}} \in_{\mathcal{R}} \mathbb{Z}_q$ et en rendant disponible sa clé publique $y_{\mathcal{T}} = g_2^{x_{\mathcal{T}}}$. Ces étapes sont résumées à la figure 7.1.

1° $\mathcal{B}$ détermine et rend disponible (g, g_1, g_2, g_3), des générateurs de $\mathbb{Z}_q$.

2° $\mathcal{B}$ choisit $x \in_{\mathcal{R}} \mathbb{Z}_q$ et calcule sa clé publique $y = g^x$.

3° $\mathcal{T}$ choisit sa clé privée $x_{\mathcal{T}} \in_{\mathcal{R}} \mathbb{Z}_q$.

4° $\mathcal{T}$ rend disponible sa clé publique $y_{\mathcal{T}} = g_2^{x_{\mathcal{T}}}$.

FIG. 7.1 - *Procédé révocable : initialisation du système par le fiduciaire*

L'idée fondamentale est que $\mathcal{U}$ doit fournir à $\mathcal{B}$ une certaine information au cours des protocoles de retrait et de dépôt, information que $\mathcal{B}$ peut inclure dans ses registres. Cette information est telle que $\mathcal{T}$ peut facilement la dévoiler à l'aide de sa clé privée.

Dans le protocole de retrait de la figure 7.2, on voit que le message m est légèrement modifié et correspond dorénavant à $m = (I \cdot g_2 \cdot g_3^t)$, où $t \equiv s^{-1} \pmod q$. Ceci implique qu'il diffère pour chaque exécution du protocole, puisque $\mathcal{U}$ choisit un masque s neuf à chaque nouveau retrait. La signature à l'aveugle restrictive reste inchangée car, au début du protocole, $\mathcal{U}$ connaît une représentation $(u_1, 1, t)$ de m par rapport à (g_1, g_2, g_3), alors qu'à la fin, il connaît la représentation $(u_1 s, s, 1)$ de A par rapport à (g_1, g_2, g_3).

$\mathcal{U}$ démontre alors à $\mathcal{B}$ qu'il utilise le même s pour masquer la clé publique de $\mathcal{T}$ que pour masquer m : il y arrive en calculant $m = (I \cdot g_2 \cdot g_3^t)$, en masquant la clé publique de $\mathcal{T}$, c'est-à-dire en calculant $\widetilde{y}_{\mathcal{T}} = y_{\mathcal{T}}^s$ et en engageant ensuite avec $\mathcal{B}$ un protocole de preuve interactive du type de celui de la figure 2.3, où il démontre à $\mathcal{B}$ que

$$\log_{g_3} m/Ig_2 = \log_{\widetilde{y}_{\mathcal{T}}} y_{\mathcal{T}},$$

avec pour effet de convaincre $\mathcal{B}$ que la clé publique de $\mathcal{T}$ a bel et bien été masquée à l'aide de s.

De plus, pour les besoins du protocole de paiement, on sépare B en B_1, B_2 tels que $B = B_1 \cdot B_2$. La signature est alors un tuplet (A, B_1, B_2, σ), $\sigma = (z, a, b, r)$, tel que pour $d = H(A, B_1, B_2, z, a, b)$,

$$\begin{aligned} g^r &= a \cdot y^d, \\ A^r &= b \cdot z^d. \end{aligned}$$

$\mathcal{U}$		$\mathcal{B}$
$s \in_{\mathcal{R}} \mathbb{Z}_q, t \leftarrow s^{-1} \bmod q$		
$m \leftarrow I \cdot g_2 \cdot g_3^t$		
$\widetilde{y}_{\mathcal{T}} \leftarrow y_{\mathcal{T}}^s$		
	$\xrightarrow{m, \widetilde{y}_{\mathcal{T}}}$	
Prouve à $\mathcal{B}$ que :		
$\log_{g_3} m/(Ig_2) = \log_{\widetilde{y}_{\mathcal{T}}} y_{\mathcal{T}}$		
$\vdots$	$\vdots$	$\vdots$
$x_1, x_2 \in_{\mathcal{R}} \mathbb{Z}_q$		
$B_1 \leftarrow g_1^{x_1}, B_2 \leftarrow g_2^{x_2}$		
$d \leftarrow H(A, B_1, B_2, z, a, b)$		
$\vdots$	$\vdots$	$\vdots$
(A, B_1, B_2, σ)		$(m, \widetilde{\sigma}, \widetilde{y}_{\mathcal{T}})$

FIG. 7.2 - *Procédé révocable : protocole de retrait*

Pour effectuer un achat, $\mathcal{U}$ et $\mathcal{S}$ exécutent le protocole de la figure 7.3 ; $\mathcal{U}$ exhibe une paire (A, B) de même qu'une signature σ telle que $ver(A, B, \sigma) = vrai$. La valeur A est cependant calculée en deux parties séparées $A_1 = g_1^{u_1 \cdot s}$ et $A_2 = g_2^s$, car la quantité A_2 doit être explicitement transmise à $\mathcal{B}$ au cours du protocole. Pour cette raison, le protocole n'est plus une preuve interactive que $\mathcal{U}$ connaît une représentation de A et de B par rapport à (g_1, g_2, g_3), mais plutôt deux preuves interactives, exécutées en parallèle, que $\mathcal{U}$ connaît le logarithme $\log_{g_1}(A_1 B_1) = u_1 \cdot s + x_1$ ainsi que le logarithme $\log_{g_2}(A_2 B_2) = s + x_2$.

$$
\begin{array}{lcr}
\mathcal{U}(A, B_1, B_2, \sigma) & & \mathcal{S}(g_3) \\
\hline
A_1 \leftarrow g_1^{u_1 \cdot s} & & \\
A_2 \leftarrow g_2^{s} & & \\
 & \xrightarrow{A, B_1, B_2, \sigma, A_1, A_2} & A = A_1 \cdot A_2 \cdot g_3 \ ? \\
 & & ver(A, B_1, B_2, \sigma) = \textbf{vrai} \, ? \\
 & & d \in_{\mathcal{R}} \mathbb{Z}_q \\
r_1 \leftarrow d(u_1 \cdot s) + x_1 \bmod q & \xleftarrow{d} & \\
r_2 \leftarrow ds + x_2 \bmod q & & \\
 & \xrightarrow{r_1, r_2} & g_1^{r_1} = A_1^d \cdot B_1 \, ? \\
 & & g_2^{r_2} = A_2^d \cdot B_2 \, ? \\
\hline
 & & (A, B_1, B_2, A_1, A_2, \sigma, r_1, r_2)
\end{array}
$$

FIG. 7.3 - *Procédé révocable : protocole d'achat*

7.1.1 Identifier un individu

À partir de la transcription du protocole de dépôt d'une pièce donnée, il est maintenant facile d'identifier l'individu qui l'a obtenue lors d'un retrait (figure 7.4) : $\mathcal{T}$ est en mesure de déterminer $\widetilde{y}_{\mathcal{T}}$ à partir de la quantité A_2 transmise au cours du dépôt. $\mathcal{B}$ peut alors retrouver cette quantité dans ses transcriptions de protocoles de retrait. [10]

10. Par souci d'efficacité, DAVIDA, FRANKEL, TSIOUNIS et YUNG (1997) proposent une méthode permettant d'effectuer cette recherche dans le registre des comptes de $\mathcal{B}$, plutôt que dans le registre global des retraits, beaucoup plus volumineux.

1º $\mathcal{B}$ envoie à $\mathcal{T}$ une transcription du protocole de dépôt.

2º $\mathcal{T}$ calcule $A_2^{x_\mathcal{T}} = g_2^{s \cdot x_\mathcal{T}} = y_\mathcal{T}^s = \widetilde{y}_\mathcal{T}$ et le transmet à $\mathcal{B}$.

3º $\mathcal{B}$ cherche $\widetilde{y}_\mathcal{T}$ dans son registre des retraits.

FIG. 7.4 - *Procédé révocable : retracer un individu avec l'aide du fiduciaire*

7.1.2 Identifier une pièce

À partir de la transcription d'un protocole de retrait donné, il est maintenant facile de retracer le parcours d'une pièce à travers le système (figure 7.5) : $\mathcal{T}$ est en mesure de dévoiler la quantité $\widetilde{y}_\mathcal{T}$, qui n'est autre que la quantité A_2 apparaissant dans le registre de dépôts de $\mathcal{B}$.

1º $\mathcal{B}$ envoie à $\mathcal{T}$ une transcription du protocole de retrait.

2º $\mathcal{T}$ calcule $\widetilde{y}_\mathcal{T}^{(x_\mathcal{T})^{-1}} = g_2^s = A_2$ et le transmet à $\mathcal{B}$.

3º $\mathcal{B}$ peut maintenant retrouver A_2 dans son registre de dépôts.

FIG. 7.5 - *Procédé révocable : retracer une pièce avec l'aide du fiduciaire*

* * *

Au cours des derniers chapitres, nous avons examiné en quelque détail les problématiques entourant la protection de la vie privée et les différents niveaux de protection offerts tant aux individus qu'aux institutions. Nous étudions à présent des caractéristiques beaucoup plus prosaïques, qui auront cependant un impact important sur l'acceptation à grande échelle de la monnaie électronique : la capacité à effectuer des paiements, efficacement et avec flexibilité.

Chapitre 8

Divisibilité et transférabilité

« A million dollars in $20 bills weighs 111 pounds, in $5 bills 444 pounds. »
OFFICE OF TECHNOLOGY ASSESSMENT, *Money Laundering*

Un mécanisme de paiement qui vise à être adopté sur une grande échelle par les consommateurs doit tenir compte du fait que les activités commerciales d'un individu économiquement actif sont souvent extrêmement diversifiées. En particulier, celui-ci :

1° engage des transactions avec des entités dont la nature va du simple commerce aux institutions gouvernementales, en passant par les amis ;

2° règle des paiements de valeurs très variables, mais désire interagir le moins souvent possible avec l'institution émettrice.

Le papier-monnaie résout ces deux problématiques de façon particulièrement élégante. La première, par le simple fait qu'il ne distingue pas entre consommateur et marchand : le transfert de fonds peut s'effectuer tout aussi bien dans une direction que dans l'autre, faisant du papier-monnaie un outil exceptionnellement flexible pour réaliser l'échange de biens et services. La seconde, grâce au protocole selon lequel les marchands acceptent d'être payés un montant supérieur et rendent ensuite la monnaie sur le trop-perçu.

Dans les deux cas, l'on utilise de façon implicite la *transférabilité* du papier-monnaie. Cette propriété, qui nous semble naturelle et évidente, comporte cependant de nombreux inconvénients dans le contexte de la monnaie électronique, comme nous le découvrirons à la section suivante ; pour ces raisons, la littérature a également exploré la notion de *divisibilité*, qui fait l'objet de la section 8.2. Nous effectuons finalement un bref survol des autres méthodes proposées dans le but d'améliorer l'efficacité des procédés de monnaie électronique.

8.1 Transférabilité

Définition 8.1.1 Un procédé de monnaie électronique est dit *transférable* si une entité $\mathcal{P}$, ayant obtenu une pièce de monnaie par l'exécution d'un protocole de paiement avec une entité $\mathcal{Q}$, peut la dépenser par une exécution du protocole de paiement avec une entité $\mathcal{R}$, sans devoir recourir à la banque entre les deux transactions.

Pour être qualifié de transférable, un procédé doit permettre d'effectuer au moins un transfert par pièce ; le parcours d'une pièce, que nous avions jusqu'à présent fixé à

$$\mathcal{B} \longrightarrow \mathcal{U} \longrightarrow \mathcal{S} \longrightarrow \mathcal{B}$$

correspond alors à

$$\mathcal{B} \longrightarrow \mathcal{U}_i \longrightarrow \mathcal{S}_i \longrightarrow \ldots \longrightarrow \mathcal{U}_j \longrightarrow \mathcal{S}_j \longrightarrow \mathcal{B}.$$

Dans la logique des procédés en différé, l'intérêt de cette propriété est immédiat : plus la chaîne de transferts est longue, plus le nombre d'exécutions de protocoles de dépôt avec $\mathcal{B}$ est réduit, permettant de réduire d'autant l'engorgement du réseau et des ressources de la banque. [1]

La notion de transférabilité a reçu peu d'attention dans la littérature [2], principalement suite aux travaux de CHAUM et PEDERSEN (1992a) : ces derniers ont démontré que la transférabilité présente des inconvénients importants dans le contexte d'un procédé de monnaie électronique en différé, anonyme et avec détection de la réutilisation (comme celui présenté à la section 5.2), inconvénients illustrés à la section qui suit.

8.1.1 Ajouter la transférabilité

Nous présentons ici une technique simple, due à VAN ANTWERPEN (1990), permettant d'ajouter une transférabilité limitée (un transfert par pièce) aux procédés que nous avons déjà définis. La généralisation à un nombre arbitraire de transferts par pièce se déduit immédiatement.

Nous utilisons une fois de plus le procédé de Brands (section 5.2) : on se souvient que la banque dispose d'une clé secrète x et que $\mathcal{U}$ peut dépenser une pièce (A, B, σ) si $ver(A, B, \sigma) = vrai$ et s'il connaît une représentation de A et de B par rapport aux générateurs (g_1, g_2). Pour réaliser la transférabilité, $\mathcal{B}$ doit également disposer d'un procédé

1. Évidemment, tout procédé transférable est nécessairement en différé.
2. Dans la pratique aussi, selon un rapport de la Banque des Règlements Internationaux (1996) : « *The Task Force found that free transferability, in which customers, merchants or banks may make unlimited direct transfers between one another, is a theoretical concept only.* »

de signature à l'aveugle avec fonctions de signature et de vérification ($\overline{sig}$, $\overline{ver}$), signature utilisée à la seule fin d'encoder l'identité des utilisateurs qui s'échangent une pièce le long de la chaîne de transferts.

Soit un usager $\mathcal{Q}$ et son secret u_0 ; nous illustrons le processus de transfert d'une pièce (A, B, σ), $A = (g_1^{u_0} \cdot g_2)^s$ de $\mathcal{Q}$ à un usager $\mathcal{R}$ qui l'utilise ensuite pour un paiement à un commerçant $\mathcal{S}$. L'usager $\mathcal{R}$ a obtenu de $\mathcal{B}$ un ensemble de triplets $\{(A_{\mathcal{R}}, B_{\mathcal{R}}, \sigma_{\mathcal{R}})\}$ tels que $\overline{ver}(A_{\mathcal{R}}, B_{\mathcal{R}}, \sigma_{\mathcal{R}}) = vrai$. Ces pièces sont en tout point identiques à des pièces que $\mathcal{R}$ pourrait obtenir par l'exécution d'un protocole de retrait avec $\mathcal{B}$, à la seule différence qu'elles sont signées par $\mathcal{B}$ à l'aide de sa fonction de signature $\overline{sig}$. Ces pseudo-pièces ont pour fonction d'encoder l'identité de $\mathcal{R}$ au sein des pièces qui lui sont transférées par $\mathcal{Q}$, ce qui permettra à $\mathcal{B}$ d'identifier correctement qui, de $\mathcal{Q}$ ou de $\mathcal{R}$, a réutilisé la pièce, le cas échéant.

Soit la pseudo-pièce $(A_{\mathcal{R}}, B_{\mathcal{R}}, \sigma_{\mathcal{R}})$, $A_{\mathcal{R}} = (g_1^{u_1} \cdot g_2)^s$, *i. e.* elle encode le secret u_1 de $\mathcal{R}$ et celui-ci a utilisé le masque s. Le transfert d'une pièce (A, B, σ) de $\mathcal{Q}$ à $\mathcal{R}$ est illustré à la figure 8.1. Le protocole est identique à celui de la figure 5.3, à la seule différence que

$\mathcal{Q}(A, B, \sigma)$		$\mathcal{R}(A_{\mathcal{R}}, B_{\mathcal{R}}, \sigma_{\mathcal{R}})$
$\vdots$	$\vdots$	$\vdots$
		$d \leftarrow H(A_{\mathcal{R}}, B_{\mathcal{R}})$
$\vdots$	$\vdots$	$\vdots$
		$(A, B, \sigma, d, q_1, q_2), (A_{\mathcal{R}}, B_{\mathcal{R}}, \sigma_{\mathcal{R}})$

FIG. 8.1 - *Transfert d'une pièce entre deux utilisateurs*

$\mathcal{R}$ calcule le défi d comme $d = H(A_{\mathcal{R}}, B_{\mathcal{R}})$, plutôt que de le choisir aléatoirement, dans le but d'encoder son identité au sein de la pièce. À la fin du protocole, $\mathcal{R}$ dispose de la paire de points (q_1, q_2), obtenue de $\mathcal{Q}$ en réponse au défi d de $\mathcal{R}$.

Le protocole de paiement entre $\mathcal{R}$ et $\mathcal{S}$ utilisant la pièce (A, B, σ) est illustré à la figure 8.2. Il correspond également à celui de la figure 5.3, si ce n'est que $\mathcal{S}$ doit dorénavant vérifier les signatures sur les deux triplets (A, B, σ) et $(A_{\mathcal{R}}, B_{\mathcal{R}}, \sigma_{\mathcal{R}})$.

Si $\mathcal{Q}$ dépense deux fois la pièce (A, B, σ), alors $\mathcal{B}$ obtiendra deux paires de points (q_1, q_2) et (q_1', q_2') tels que

$$u_0 = \frac{(q_1 - q_2)}{(q_1' - q_2')}$$

$\mathcal{R}(A, B, \sigma, q_1, q_2), (A_{\mathcal{R}}, B_{\mathcal{R}}, \sigma_{\mathcal{R}})$		$\mathcal{S}$
	$\xrightarrow{A, B, \sigma, q_1, q_2}$	
	$\xrightarrow{A_{\mathcal{R}}, B_{\mathcal{R}}, \sigma_{\mathcal{R}}}$	
		$ver(A, B, \sigma)$ = **vrai** ? $d \leftarrow H(A_{\mathcal{R}}, B_{\mathcal{R}})$ $g_1^{q_1} \cdot g_2^{q_2} = A^d \cdot B$? $d' \in_{\mathcal{R}} \mathbb{Z}_q$
$r_1 \leftarrow d'(u_1 \cdot s) + x_1 \bmod q$ $r_2 \leftarrow d's + x_2 \bmod q$	$\xleftarrow{d'}$	
	$\xrightarrow{r_1, r_2}$	$\overline{ver}(A_{\mathcal{R}}, B_{\mathcal{R}}, \sigma_{\mathcal{R}})$ = **vrai** ? $g_1^{r_1} \cdot g_2^{r_2} = A_{\mathcal{R}}^{d'} \cdot B_{\mathcal{R}}$?
		$(A, B, \sigma, d, q_1, q_2)$, $(A_{\mathcal{R}}, B_{\mathcal{R}}, \sigma_{\mathcal{R}}, d', r_1, r_2)$

FIG. 8.2 - *Procédé transférable : protocole de paiement*

avec lesquels déterminer son identité, alors que si $\mathcal{R}$ dépense deux fois la pièce, $\mathcal{B}$ obtiendra deux paires de points tels que

$$u_1 = \frac{(r_1 - r_2)}{(r_1' - r_2')}.$$

Cette méthode illustre bien les difficultés inhérentes à l'ajout de la transférabilité au sein d'un procédé en différé, anonyme, avec détection de la réutilisation. La première de ces difficultés — et la plus sérieuse — est que la monnaie « grossit » avec chaque transfert : on ne peut conserver les caractéristiques de détection de la réutilisation sans encoder dans la pièce l'identité de chaque entité participant à la chaîne de transferts. Pour un procédé donné, le nombre de transferts possibles est donc nécessairement limité. De plus, la banque se doit d'inscrire dans ses registres une pièce supplémentaire par transfert : dans notre exemple, elle doit conserver non seulement (A, B, σ, q_1, q_2), qui détermine l'identité de $\mathcal{Q}$, mais aussi $(A_{\mathcal{R}}, B_{\mathcal{R}}, \sigma_{\mathcal{R}}, r_1, r_2)$, qui détermine l'identité de $\mathcal{R}$. La taille du registre s'accroit donc linéairement avec le nombre de transferts permis par pièce.

De plus, $\mathcal{U}$ est désormais à même de reconnaître une pièce qui lui est déjà passée entre les mains *(forward-traceability)*. Ceci représente une qualité d'anonymat plus faible que ce que nous avions obtenu jusqu'à présent, puisque dans un système où le nombre de transferts est limité, $\mathcal{U}$ peut alors déduire certaines informations sur le parcours de la pièce.

Les procédés de monnaie électronique se mesurent donc fort peu avantageusement à un système aussi souple que le papier-monnaie, où un billet peut circuler au sein du système sans jamais repasser par une banque, tout en assurant l'anonymat à chacun de ses utilisateurs ! Fort heureusement, il est possible de limiter les dommages : si les transactions semblent devoir rester limitées au triangle plus ou moins élargi $\mathcal{B}$, $\mathcal{U}$ et $\mathcal{S}$, d'autres méthodes existent pour permettre à $\mathcal{U}$ d'acquitter ses factures sans pour autant se promener les poches pleines de petite monnaie électronique.

8.2 Divisibilité

Jusqu'à ce point, nous avons évité d'aborder de front le problème de la petite monnaie, en présumant implicitement qu'à chaque pièce est associée une certaine valeur et que l'usager dispose d'un grand nombre de pièces de chaque dénomination pour effectuer ses paiements, tel que précisé à la section 3.8. Ceci ne représente pas vraiment une solution satisfaisante au problème du paiement efficace de valeurs diverses, puisqu'elle fait entièrement reposer la charge du problème sur le consommateur, qui doit être toujours muni de la monnaie exacte et, pour ce faire, effectuer un grand nombre de retraits à la banque afin de garnir son portefeuille. Une solution possible est d'utiliser des pièces divisibles :

Définition 8.2.1 Une pièce *divisible* de valeur w\$ est une pièce qui peut être dépensée plusieurs fois, en autant que la valeur totale des transactions où elle est utilisée ne dépasse pas w\$.

Si les monnaies fiduciaires modernes sont rarement divisibles, il est par contre souvent facile de diviser les monnaies-marchandises : les cigarettes utilisées comme moyen d'échange par les soldats au cours de la Seconde Guerre mondiale sont un bon exemple.

La notion de divisibilité a surtout été explorée par Tastuami Okamoto (OKAMOTO et OHTA 1990, 1992 ; OKAMOTO et ENG 1994 ; OKAMOTO 1995).[3] Nous explorons un des mécanismes qu'il a imaginés et qui présente l'avantage de s'intégrer parfaitement au procédé décrit à la section 5.2.

3. JAKOBSSON (1995b) s'est aussi intéressé à la notion de divisibilité de la monnaie mais sous un tout autre angle : celui de *déchirer* un billet en deux morceaux, dans le but d'assurer un échange équitable lors d'une transaction entre deux parties.

8.2.1 La technique d'Okamoto

Les procédés conçus par Okamoto utilisent tous l'idée d'encoder une pièce c par une arborescence binaire[4] : à une pièce de valeur $w = 2^\ell$ est associé une arborescence binaire de $1 + \ell$ niveaux et de w feuilles. La racine de l'arbre est notée n_0 ; son enfant gauche est noté n_{00} alors que son enfant droit est noté n_{01} ; l'enfant gauche d'un nœud n_{0v} situé au niveau i, $|v| = i$, est noté n_{0v0} alors que son enfant droit est noté n_{0v1}. À chaque nœud de l'arbre est associée une certaine dénomination : la racine n_0 a pour valeur w, alors qu'un nœud au niveau i a pour valeur $w/2^i$; en particulier, les feuilles de l'arbre ont pour valeur $w/2^\ell = 1$. La situation est illustrée à la figure 8.3.

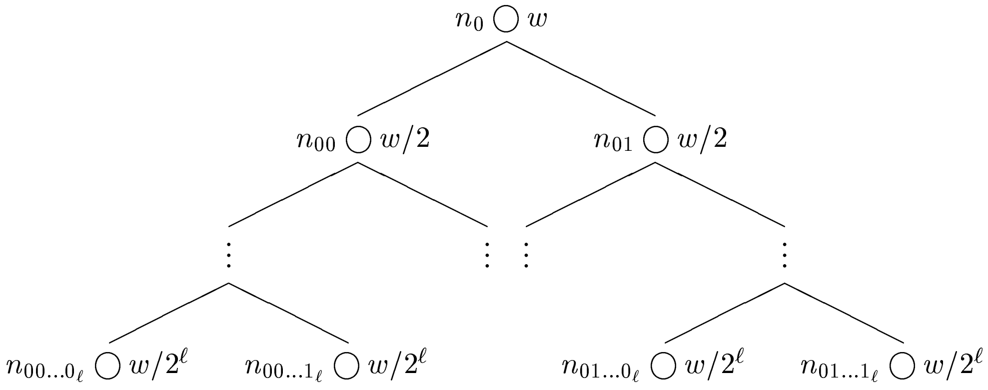

FIG. 8.3 - *Structure d'une pièce divisible*

L'idée principale est que la divisibilité peut être réalisée de façon sécuritaire en observant les deux règles suivantes :

1° *Parcours unique :* Lorsqu'un nœud est utilisé, aucun de ses descendants ni de ses ancêtres ne peut être utilisé.

2° *Nœud unique :* Aucun nœud ne peut être utilisé plus d'une fois.

Dans le procédé d'Okamoto, utiliser une pièce pour des transactions d'une valeur totale supérieure à w\$ ou dépenser deux fois toute portion de la pièce implique nécessairement de violer l'une de ces deux règles.

Lorsque $\mathcal{U}$ désire dépenser un certain montant de sa pièce (disons $w/2^k$), il révèle par la même occasion un point sur la ligne — selon les techniques maintenant familières de la section 5.1 — dont les coefficients sont encodés dans le nœud correspondant à $w/2^k$. Il révèle également les coefficients encodés dans tous les descendants et

4. Nous présentons l'encodage décrit par OKAMOTO et ENG (1994), puisqu'il s'intègre parfaitement avec le procédé de Brands ; OKAMOTO (1995) présente des résultats plus satisfaisants en termes d'efficacité de transfert et de calculs, mais demeure relativement complexe.

tous les ancêtres de ce nœud : si l'un de ces nœuds est réutilisé, $\mathcal{B}$ pourra facilement déterminer l'identité de $\mathcal{U}$.

8.2.2 Calcul des valeurs de chaque nœud

Soit $\mathbb{Z}_q$, un groupe d'ordre q tel que le calcul des logarithmes discrets y est réputé difficile, soit $H_{2|q|} : \{0,1\}^* \rightarrow \{0,1\}^{2|q|}$, une fonction de hachage cryptographique forte et soit une pièce divisible de valeur $w = 2^\ell$, représentée par un arbre binaire comme celui de la figure 8.3. On associe certaines valeurs à chaque nœud, en procédant de manière ascendante, des feuilles jusqu'à la racine. Ces valeurs, notées t, r^1 et r^2, sont définies de la façon suivante :

Pour une feuille $n_{0\ldots j_\ell}, j_\ell \in \{0,1\}$ et un germe secret e choisit aléatoirement par $\mathcal{U}$,

$$t_{0\ldots j_\ell} = H_{2|q|}(e \mid\mid 0 \ldots j_\ell)$$

et

$$t_{0\ldots j_\ell} = r^1_{0\ldots j_\ell} \mid\mid r^2_{0\ldots j_\ell},$$

c'est-à-dire que $r^1_{0\ldots j_\ell}$ correspond aux q bits les plus significatifs de la représentation binaire de $t_{0\ldots j_\ell}$ alors que $r^2_{0\ldots j_\ell}$ correspond à ses q bits les moins significatifs.

Pour un nœud interne, les valeurs t, r^1 et r^2 d'un nœud sont calculées à partir de ses enfants ; ainsi, pour un nœud $n_{0\ldots j_k}, j_k \in \{0,1\}, 1 \leq k \leq \ell - 1$, dont l'enfant gauche a pour valeurs t, r^1 et r^2 :

$$t_{0\ldots j_k 0} = r^1_{0\ldots j_k 0} \mid\mid r^2_{0\ldots j_k 0},$$

et l'enfant droit :

$$t_{0\ldots j_k 1} = r^1_{0\ldots j_k 1} \mid\mid r^2_{0\ldots j_k 1},$$

les valeurs t, r^1 et r^2 du nœud sont :

$$t_{0\ldots j_k} = H_{2|q|}\left(H_{2|q|}(g_1^{r^1_{0\ldots j_k 0}} \cdot g_2^{r^2_{0\ldots j_k 0}}) \mid\mid H_{2|q|}(g_1^{r^1_{0\ldots j_k 1}} \cdot g_2^{r^2_{0\ldots j_k 1}})\right).$$

Les valeurs t, r^1 et r^2 de chacun des nœuds de l'arbre sont ainsi définies, jusqu'aux valeurs t_0, r^1_0 et r^2_0 de la racine.

8.2.3 Retrait d'une pièce

Le protocole de retrait d'une pièce est presque identique à celui de la section 5.2 : une pièce est définie comme un triplet (A, B, σ). Si un consommateur connaît une représentation de A et de B par rapport à (g_1, g_2), on dit qu'il connaît une représentation de la pièce et dépenser une pièce exige qu'il démontre la possession de telles représentations. Dans le protocole 5.2, la représentation de A est $(u_1 s, s)$ où u_1 est l'identité de $\mathcal{U}$, et la représentation de B est choisie aléatoirement comme $(x_1, x_2) \in_{\mathcal{R}} \mathbb{Z}_q$ *i. e.* $B = g_1^{x_1} \cdot g_2^{x_2}$. Pour intégrer la technique de divisibilité d'Okamoto, il suffit de choisir la représentation de B comme r_0^1 et r_0^2, c'est-à-dire les valeurs r^1 et r^2 de la racine de l'arbre.

8.2.4 Protocole de paiement

Tout d'abord, tout comme au protocole de la figure 5.3, $\mathcal{U}$ exhibe la pièce (A, B, σ) à $\mathcal{S}$ qui s'assure que $\mathit{ver}(A, B, \sigma) = \mathit{vrai}$. $\mathcal{U}$ révèle ensuite la contribution du nœud $n_{0\ldots j_k}$ au calcul des valeurs t de ses ancêtres, en calculant

$$\beta_{0\ldots j_k} = g_1^{r^1_{0\ldots j_k}} \cdot g_2^{r^2_{0\ldots j_k}} \bmod p$$

et en révélant

$$\begin{array}{l} H_{2|q|}\left(g_1^{r^1_{0\ldots\overline{j_k}}} \cdot g_2^{r^2_{0\ldots\overline{j_k}}}\right), \\ H_{2|q|}\left(g_1^{r^1_{0\ldots\overline{j_{k-1}}}} \cdot g_2^{r^2_{0\ldots\overline{j_{k-1}}}}\right), \\ \vdots \\ H_{2|q|}\left(g_1^{r^1_{0\ldots\overline{j_2}}} \cdot g_2^{r^2_{0\ldots\overline{j_2}}}\right), \\ H_{2|q|}\left(g_1^{r^1_{0\overline{j_1}}} \cdot g_2^{r^2_{0\overline{j_1}}}\right), \end{array}$$

où la notation $\overline{a}$ désigne la complémentation d'un bit a. À partir de ces informations, $\mathcal{S}$ est en mesure de calculer les valeurs t, r^1 et r^2 de chacun des ancêtres directs du nœud $n_{0\ldots j_k}$, jusqu'aux valeurs t_0, r_0^1 et r_0^2 de la racine.

Le marchand $\mathcal{S}$ choisit ensuite un défi $d \in_{\mathcal{R}} \mathbb{Z}_q$ qu'il transmet à $\mathcal{U}$. Celui-ci présente alors

$$y_1 = r^1_{0\ldots j_k} + d \cdot (u_1 \cdot s) \bmod q, \tag{8.1}$$

$$y_2 = r^2_{0\ldots j_k} + d \cdot s \bmod q, \tag{8.2}$$

et $\mathcal{S}$ vérifie que

$$g_1^{y_1} \cdot g_2^{y_2} \equiv \beta_{0\ldots j_k} \cdot A^d \pmod q.$$

Nous avons déterminé que de dépenser deux nœuds sur un même parcours de la racine jusqu'à une feuille constituait une sur-utilisation de la pièce. En effet, il est clair que si $\mathcal{U}$ tente de dépenser deux fois le même nœud, $\mathcal{B}$ obtient deux paires (y_1, y_2) et (y_1', y_2') de points à partir desquels il peut déterminer u_1 de la même façon qu'à la section 5.1.

Si deux nœuds distincts n_a et n_b sur le même parcours sont dépensés, alors l'identité de $\mathcal{U}$ sera révélée : en effet, si n_a est le nœud le plus éloigné de la racine, nous disposons alors des valeurs t, r^1 et r^2 de n_b. Ceci, avec les points y_1 et y_2 obtenus lorsque n_b fut dépensé, nous permet de résoudre les équations 8.1 et 8.2 pour s et u_1, obtenant du même coup l'identité de $\mathcal{U}$.

Évidemment, le coût calculatoire et la quantité d'information transmise lors du protocole de paiement sont accrus : celle-ci est de l'ordre de $\log \mathcal{N}$, où $\mathcal{N}$ = (la valeur totale de la pièce)/(la plus petite valeur divisible de la pièce). De plus, la taille de la pièce augmente linéairement avec $\mathcal{N}$.

Un inconvénient important des procédés de monnaie divisible est que pour pouvoir détecter la réutilisation, la banque doit conserver des informations qui lui permettent de relier facilement chaque fraction de pièce dépensée à la même pièce (les valeurs t_0, r_0^1 et r_0^2 seront les mêmes pour chacune des fractions d'une même pièce). La propriété de non-corrélation des paiements dont jouissaient nos procédés jusqu'à ici se trouve ainsi affaiblie. Ce problème demeure ouvert, puisqu'à ce jour aucun mécanisme de divisibilité des pièces n'a été conçu qui assure la non-corrélation des paiements effectués à partir d'une même pièce.

8.3 Autres approches

À l'heure actuelle, les méthodes qui permettraient la conception de procédés de monnaie électronique à la fois flexibles et efficaces font tout simplement défaut. L'univers du commerce électronique semble être condamné à devoir offrir une variété de mécanismes de paiement adaptés à des besoins spécifiques. Nous examinons ici quelques-unes des solutions proposées dans la littérature.

L'idée de *chèques électroniques* a initialement été proposée par CHAUM, FIAT et NAOR (1988) et subséquemment explorée par DEN BOER *et al.* (1990), HIRSCHFELD (1993) et BRANDS (1994b). Ces chèques peuvent être utilisés pour payer n'importe quel montant inférieur à une certaine limite et ensuite retournés à la banque pour un remboursement de leur portion inutilisée ; en plus des protocoles de retrait, d'achat et de dépôt, ces procédés comportent donc un protocole supplémentaire de *remboursement*.

À partir de son procédé décrit à la section 5.2, Brands a proposé un modèle hybride — mi-chèque, mi-monnaie — nécessitant un module inviolable (BRANDS 1994a ; 1995) : l'usager retire en une seule opération un montant global de son compte à la banque, de même qu'un certain nombre de « certificats » qui peuvent être dépensés pour des montants de valeur arbitraire, jusqu'à concurrence du montant global maintenu en mémoire du module. Brands propose de combiner ces certificats avec des pièces dans le but d'obtenir une procédure de paiement relativement efficace : un montant de 16,39 $, par exemple, pourrait être réglé à l'aide d'une pièce de 10,00 $, une pièce de 5,00 $ et un certificat bon pour 1,39 $, éliminant ainsi la menue monnaie encombrante.

Certains types particuliers de paiement sont aussi considérés : BRANDS (1994b) montre comment transformer son système de pièces — *one-show credentials* — en un système de tickets — *k-show credentials* — pouvant être exhibés *k* fois pour effectuer des paiements de valeur identique.

* * *

Une forme particulière de paiement est appellée à prendre un essor important, parallèlement au développement des nouvelles formes de perception du droit d'auteur rendues possibles par l'avènement des réseaux électroniques à grande échelle : le *micropaiement* semble promis à un avenir si brillant que nous lui consacrons le prochain chapitre.

Chapitre 9

Les micropaiements

Si les procédés de monnaie électronique ont suscité un tel intérêt depuis quelques années, c'est sans nul doute dû à l'essor sans précédent des réseaux électroniques internationaux et au potentiel commercial s'y rattachant. Un des marchés rendu possible par le déploiement à grande échelle de ces réseaux consiste en des services de consultation d'œuvres — journaux, ouvrages, photos, musique, vidéo, événements artistiques — facturés à l'utilisation, [1] mais selon une grille beaucoup plus fine qu'il n'était possible auparavant. Les grandes entreprises s'affairent actuellement à mettre au point les interfaces qui permettront d'accéder à ces œuvres et de simultanément s'acquitter des droits d'auteur afférents. Ces droits d'auteur seront probablement de petite valeur, de l'ordre de quelques cent peut-être pour la consultation d'un article, la recherche d'une référence ou l'audition d'une œuvre musicale. Nous désignerons l'unité de valeur de ces paiements par un *tic*. [2]

Les mécanismes de paiement électronique à même de réaliser de telles transactions se regroupent essentiellement en trois catégories :

1° *Comptes privilégiés* : Un client établit un compte privilégié auprès de chaque fournisseur de services avec qui il fait affaire, celui-ci ne le facturant qu'une fois par mois ; cette approche a l'inconvénient d'imposer une relation à long terme entre client et fournisseur, ce qui ne correspond pas aux relations éphémères qui pourraient caractériser ce nouveau marché ;

2° *Cartes de crédits* : Si cette méthode a le mérite d'être bien établie et de disposer d'une infrastructure étendue déjà opérationnelle, elle nécessite cependant

---

1. *Pay-per-view*.

2. Cette terminologie est due à PEDERSEN (1995) qui s'inspire du contexte des appels téléphoniques (on parle ici du contexte européen) : le montant total à payer est composé de plusieurs paiements de petite valeur, chacun de ces minuscules montants devant être payé en temps réel, sur réception d'un *tic*. Selon le type d'appel (local ou interurbain), les tics sont reçus à des intervalles plus ou moins rapprochés.

d'obtenir l'autorisation d'une organisation centrale lors de chaque transaction. Les institutions émettrices de cartes de crédit offrent de plus de nombreux services additionnels — assurances, comptabilisation individuelle de chaque achat, protection contre la fraude — qui ajoutent inutilement au coût des transactions dans le contexte des micropaiements ;

3º *Monnaie électronique* : si la monnaie électronique offre d'excellentes garanties de sécurité, les coûts calculatoires associés à la génération et la vérification des signatures numériques sont trop importants pour que la monnaie électronique puisse servir de support aux micropaiements. Elle exige de plus que les utilisateurs obtiennent et conservent une grande quantité de pièces pour effectuer les paiements, l'équivalent électronique d'un bocal de sous noirs. Les pièces divisibles ne résolvent rien, puisque leur manipulation implique des coûts calculatoires encore plus importants.

Ces limitations apparentes des procédés de paiement conventionnels forment un obstacle au développement de services en ligne où les marchandises — articles de journaux, de magazines, références, cotes boursières — sont offertes à la pièce, pour quelques sous chacun. Pour cette raison, il semble nécessaire de développer un mécanisme de paiement spécifiquement adapté à cette situation. Nous examinons à présent une adaptation d'un procédé de monnaie électronique permettant de tels *micropaiements*.

9.1 Protocoles

Si l'on désire rendre plus efficace les procédés de monnaie électronique, il faut pouvoir diminuer le nombre d'opérations mathématiques reliées aux cryptosystèmes à clé publique (en général, l'exponentiation modulaire). Ces opérations sont autant que possible éliminées par l'utilisation de fonctions de hachage, beaucoup plus efficaces, comme l'indiquent RIVEST et SHAMIR (1996) :

> « *As a rough guide, hash functions are about 100 times faster than RSA signature verification, and about 10,000 times faster than RSA signature generation: on a typical workstation, one can sign two messages per second, verify 200 signatures per second, and compute 20,000 hash function values per second.* »

Les objectifs de sécurité d'un procédé de micropaiement sont similaires à ceux de machines distributrices ou de parcomètres par exemple : ceux-ci, sans être munis de mécanismes sophistiqués permettant la détection de fausse monnaie, conservent un niveau de fraude relativement bas. De même pour les micropaiements, la fraude à grande échelle ou à répétition doit pouvoir être détectée et éliminée, mais les abus impliquant la perte de quelques tics, tant du côté de $\mathcal{U}$ que de $\mathcal{S}$ ou de $\mathcal{B}$, importent peu.

Nous proposons d'intégrer les micropaiements à un système qui est une adaptation du procédé de Brands et que nous avons évoqué à la section 8.3. Nous n'indiquons ici que les détails les plus importants : le lecteur intéressé se référera à BRANDS (1994a). Ce système peut être décrit comme la réalisation de *chèques anonymes avec compteur* : $\mathcal{U}$ obtient lors du protocole de retrait un certain nombre de « certificats » et une permission de dépenser ces certificats jusqu'à une certaine limite, limite conservée à même la mémoire d'un module inviolable intégré au portefeuille de $\mathcal{U}$. Pour effectuer un paiement, $\mathcal{U}$ indique le montant de la transaction au module inviolable, qui le déduit de la limite. La différence avec la monnaie électronique telle que nous l'avons étudiée jusqu'à présent est que $\mathcal{U}$ peut dépenser n'importe quel montant inférieur à la limite avec un seul certificat. Si $\mathcal{U}$ parvient à briser l'inviolabilité du module, il peut dépenser un montant arbitraire avec les certificats qu'il détient, mais, comme d'habitude, il ne peut les réutiliser sans être détecté. Il est facile de réduire la portée d'un tel bris en imposant une limite supérieure au montant associé à un certificat. Comme indiqué à la section 8.3, ce type de système trouve toute son utilité lorsqu'il est combiné avec les pièces habituelles et que les certificats sont utilisés pour régler les questions de menue monnaie.

Les auteurs qui se sont intéressés aux micropaiements — PEDERSEN (1995), RIVEST et SHAMIR (1996), HAUSER, STEINER et WAIDNER (1996), GLASSMAN, MANASSE, ABADI et GAUTHIER (1995) — se sont tous inspirés des idées de Lamport pour la génération de mots de passe *jetables*[3] ; celui-ci propose l'utilisation d'une fonction de hachage cryptographique forte $H : \{0,1\}^\ell \to \{0,1\}^\ell$. La i^e application de H est notée H^i pour $i \in \mathbb{N}$, en d'autres termes H^0 dénote l'identité alors que $H^i = H \circ H^{i-1}$, pour $i = 1, 2, \ldots$

On présume qu'après avoir exécuté un protocole de retrait avec $\mathcal{B}$, $\mathcal{U}$ a obtenu des « certificats » (m, σ) tels que $ver(m, \sigma) = vrai$. Ces certificats ne correspondent à aucune dénomination particulière. Nous présumons également qu'il existe une méthode sécuritaire — décrite en détail par BRANDS (1994a) — par laquelle $\mathcal{U}$ communique à $\mathcal{S}$ un montant tel qu'il ne peut dépasser la limite inscrite à même le module inviolable et que la paire (m, σ) utilisée pour cette transaction est en quelque sorte « liée » à ce montant.

9.1.1 Paiement

Un tic est simplement une chaîne de ℓ bits, notée t. Pour effectuer un paiement à $\mathcal{S}$ d'une valeur maximale de n tics, $\mathcal{U}$ procède de la façon suivante : il choisit aléatoirement le n^e tic, $t_n \in_{\mathcal{R}} \{0,1\}^\ell$ et calcule une séquence de tics $(t_n, t_{n-1}, \ldots, t_0)$ telle que

$$t_i = H(t_{i+i}), i = n-1, \ldots, 0,$$

3. Voir MENEZES, VAN OORSCHOT et VANSTONE (1997), p. 396.

c'est-à-dire que $t_0 = H^n(t_n)$. La valeur t_0 ne correspond pas elle-même à un tic, mais plutôt à un engagement à la chaîne $t_1, \ldots, t_n$. Comme d'habitude, $\mathcal{U}$ transmet (m, σ) à $\mathcal{S}$, qui vérifie que *ver*(m, σ) = *vrai*. $\mathcal{U}$ transmet également la paire (t_0, n) à $\mathcal{S}$.

À cette étape, $\mathcal{S}$ n'a encore reçu aucun paiement pour un tic. Pour effectuer un paiement pour le i^e tick, $(i \geq 1)$, $\mathcal{U}$ transmet (t_i, i) à $\mathcal{S}$. Celui-ci peut vérifier que $H(t_i) = t_{i-1}$ à l'aide d'une seule application de la fonction de hachage H, puisque la paire $(t_{i-1}, i-1)$ a été transmise au tour précédent (les tics étant dépensés en ordre, de 1 à n). Le processus est illustré à la figure 9.1.

$\mathcal{U}(m, \sigma, n)$		$\mathcal{S}$
$t_n \in_{\mathcal{R}} \{0,1\}^\ell$		
$t_i \leftarrow H(t_{i+1}), i = n-1, \ldots, 0$		
	$\xrightarrow{m, \sigma, (t_0, n)}$	*ver*(m, σ) = **vrai** ?
$\vdots$		$\vdots$
	$\xrightarrow{(t_i, i)}$	
		$H(t_i) = t_{i-1}$?
		(t_k, k)

FIG. 9.1 - *Procédé de micropaiements : paiement du i^e tic*

Il est facile d'effectuer d'un seul coup un paiement de u tics : au i^e tour, $\mathcal{U}$ transmet t_{i+u} tel que $H^u(t_i) = t_{i-1}$. $\mathcal{S}$ doit alors effectuer u applications de la fonction de hachage afin de vérifier le paiement, alors que $\mathcal{U}$ n'effectue aucun calcul supplémentaire. Notons que pour effectuer son dépôt et se faire créditer k tics par $\mathcal{B}$, $\mathcal{S}$ n'a besoin de conserver que la paire (t_k, k) puisque, une fois que $\mathcal{U}$ a dépensé t_k, il ne peut utiliser t_i, pour $i < k$.

9.1.2 Protocole de dépôt

Pour effectuer un dépôt, $\mathcal{S}$ fournit à $\mathcal{B}$ la paire (m, σ) ainsi que la paire (t_k, k) où k est l'index du dernier tic reçu de $\mathcal{U}$. De son côté, $\mathcal{B}$ s'assure de la validité du paiement à l'aide des vérifications habituelles et vérifie que k applications de H sur t_k sont bien nécessaires pour obtenir t_0, c'est-à-dire que $t_0 = H^k(t_k)$. Le processus est illustré à la figure 9.2.

$\mathcal{S}(m, \sigma, t_k, k)$		$\mathcal{B}$
	$\xrightarrow{m, \sigma, t_0, (t_k, k),}$	
		$ver(m, \sigma)$ = **vrai** ?
		$t_0 = H^k(t_k)$?
		$m, \sigma, (t_k, k)$

FIG. 9.2 - *Procédé de micropaiements : protocole de dépôt*

* * *

Ces protocoles ne représentent qu'une des réalisations possibles du micropaiement. À l'heure actuelle, il est encore trop tôt pour prédire sous quelle forme celui-ci sera offert aux consommateurs et si les micropaiement seront intégrés aux procédés plus conventionnels de monnaie électronique, ou plutôt offerts à part. Ce survol rapide du micropaiement complète notre tour d'horizon des différentes possibilités techniques offertes par les procédés de monnaie électronique.

Chapitre 10

Conclusion

> « *Car rien n'est plus séduisant que les œuvres futures, rêvées pendant que s'achève dans la douleur un travail de longue haleine.* »
> MICHEL TOURNIER, *Le vent Paraclet*

Les chapitres précédents ont fourni, d'une part, l'occasion de s'initier aux caractéristiques techniques des procédés de monnaie électronique et, d'autre part, la démonstration que si l'*avènement* de la monnaie électronique peut être qualifié d'« inévitable », la *forme* finale que prendra cet objet technique, elle, ne l'est pas. Nous avons pu, au contraire, apprécier qu'elle résulte de jeux complexes d'influence et de pouvoir entre différents intervenants au sein du processus de design : scientifiques, gouvernements, institutions financières, processus judiciaire, etc. Bien sûr, il existe de nombreuses contraintes techniques à cette forme et c'est la nature même de notre contribution d'avoir voulu éclairer les déterminants technologiques aux formes que pourraient prendre les espèces numériques.

Libérés d'un cadre d'analyse tout aussi restrictif que complaisant, il nous est maintenant possible de nous interroger sur les mérites relatifs des objets techniques et, de façon complémentaire, sur le processus de design qui les engendre : Quels sont les objectifs de ce processus ? Quels sont les critères qui puissent nous être utiles pour juger de la qualité d'un artefact technologique ? Jusqu'à présent, nous nous sommes contenté d'appliquer les critères traditionnels du génie informatique pour évaluer les mérites relatifs des solutions offertes, c'est-à-dire l'efficacité (calculatoire et autre) de même que l'élégance mathématique d'une solution, qui, au bout du compte, caractérisent une analyse purement économique d'un objet technique. Au-delà de ces considérations, les objets techniques doivent aussi être évalués en fonction des structurations qu'ils effectuent de la vie civique, sociale, et politique de leurs utilisateurs, évaluation qui se pose avec d'autant plus de pertinence que l'on discute d'artefacts tels que la monnaie ou la signature.

Un tel ensemble de critères a été proposé par Langdon Winner, dans son superbe ouvrage *Autonomous Technology* (WINNER 1977) ; ceux-ci pourraient nous être utiles pour évaluer la qualité d'un artefact technologique, en des termes plus larges que ceux découlant d'une simple analyse économique. Ces critères sont les suivants :

Les technologies devraient être structurés de telle manière et à une telle échelle qu'elles soient intelligibles et accessibles à l'utilisateur profane.

Voilà une exigence qui semble bien idéaliste, puisque les objets qui nous entourent nous sont en majorité déjà inaccessibles intellectuellement (et, de plus en plus, physiquement) : le fonctionnement de nos voitures, de nos gadgets électroniques, de nos instruments de communication dépasse largement nos connaissances et il y a belle lurette que nous avons renoncé à appréhender autrement que superficiellement les instruments qui meublent notre quotidien.

Si l'on peut raisonnablement arguer que des connaissances en théorie des codes n'influencent en rien notre capacité à jouir de l'écoute d'un disque compact, un artefact aussi universel que la monnaie devrait être, quant à lui, le plus transparent que possible : un procédé de paiement destiné à être utilisé par le public devrait être défini de la façon la plus intelligible possible, sans présupposer un degré de sophistication technologique qui pourrait le rendre inaccessible à des groupes importants de la population. De même, les modalités d'utilisation d'un tel objet se doivent d'être aisément compréhensibles et accessibles. [1]

Les artefacts technologiques devraient être conçus de façon à offrir le maximum de flexibilité et de mutabilité.

Idéalement, le choix d'une technologie ne devrait pas imposer un carcan rigide, permanent, inflexible et irréversible aux populations d'utilisateurs. En particulier, le déploiement de l'infrastructure qui sous-tend une technologie devrait tenir compte des correctifs que l'on pourrait vouloir effectuer de façon à en atténuer les effets pervers. Ainsi, les infrastructures à clé publique requises pour le déploiement à grande échelle du commerce électronique sont des systèmes dont nous connaissons encore bien peu les modalités d'opération et dont, dans l'état actuel de nos connaissances, il est difficile de déterminer avec précision les effets. Le déploiement de telles infrastructures nécessitera des investissements importants, tant du point de vue matériel que dans l'éducation et la formation que supposent de tels changements dans nos manières de faire, et

1. Bien sûr, même l'utilisation du papier-monnaie requièrt certaines habiletés techniques, tel des rudiments d'arithmétique et d'alphabétisation, mais celles-ci sont minimes et maîtrisées par la majorité.

tant leur conception que leur réalisation devraient tenir compte de notre relative ignorance sur le déploiement à grande échelle de tels systèmes de sécurité.

Disposons-nous d'un pouvoir discrétionnaire quant à l'utilisation ou même la conception d'une technologie ?

De nos jours, la simple idée que des *limites* puissent exister au développement technologique semble relever de la pure hérésie. Ce problème se pose évidemment de façon criante dans le cas des biotechnologies, qui remettent en question nos définitions mêmes de l'être humain, de la reproduction et de la vie. Si les technologies du commerce électronique n'impliquent pas de questionnements aussi radicaux, elles fourniront néanmoins aux pouvoirs publics une occasion idéale d'établir des instruments de contrôle social, dont les effets sur notre vie civique, sociale et politique seront d'autant plus pernicieux qu'ils seront subtils. Il y a, en effet, fort à parier que les infrastructures à clé publique supposées par le commerce électronique justifieront l'instauration, sous une forme ou une autre, de « cartes d'identité nationales » de même qu'une concentration de la médiation des rapports gouvernement-citoyen par l'entremise de réseaux électroniques, toujours dans la même optique de rationalisation de l'appareil bureaucratique. Ainsi, la simple existence d'une telle ressource sera perçue comme la justification logique d'un choix de société aux ramifications importantes, celui de l'adoption d'un mécanisme universel et permanent d'identification des individus.

À la lumière de cette discussion, il est intéressant de se demander s'il existe une forme particulière du processus d'innovation qui permette d'obtenir des objets techniques se rapprochant d'avantage de ces critères. Certains chercheurs ont proposé d'utiliser ce qu'ils appellent le *design participatif*. WINNER (1977) en fait la description suivante :

> « *One major shortcoming in the technologies of the modern period is that those touched by their presence have little or no control over their design or operation. To as great an extent as possible, then, the processes of technological planning, construction, and control ought to be opened to those destined to experience the final products and full range of social consequences.* »

Le processus de développement des nouvelles technologies devrait pouvoir permettre une participation directe de ceux qui en seront les utilisateurs et en subiront les effets (anticipés ou non) : c'est à ce tournant que nous retrouvons les usagers, et la question de leur représentation et de leur mobilisation, discussion brièvement amorcée dans notre introduction à ce mémoire.

10.1 De l'usager

L'usager est à la fois le point de mire et le grand oublié du processus de design des objets techniques : simultanément glorifié et ignoré, il représente le *focus* ultime de chacun des intervenants, sans pourtant avoir réellement voix au chapitre. Une discussion du rôle de l'usager au sein du processus de design se doit d'aborder trois problématiques distinctes : 1° problème de définition, c'est-à-dire qu'avant toute chose, il s'agit de pouvoir définir cet être évanescent qu'est l'usager ; 2° problème de représentation, c'est-à-dire la façon dont chacun des groupes qui influencent le processus d'innovation technologique imagine et conçoit l'utilisateur ; 3° problème de mobilisation, c'est-à-dire la question de la représentativité des organisations qui prétendent s'exprimer au nom de l'usager.

De fait, qu'est-ce que cet usager dont nous faisons si grand cas ? Comme le souligne BOULLIER (1994), il s'agit manifestement d'un être polymorphe, puisqu'il est alternativement défini, selon le besoin, comme *utilisateur, abonné, membre, consommateur, contribuable, citoyen, lecteur, spectateur, téléspectateur, public, audience, visiteur, opinion publique, acteur* et, pour finir, *client*. Un même objet technique peut placer un utilisateur dans plusieurs modes d'utilisation : ainsi, face à une télévision, nous sommes successivement consommateurs lors d'une publicité, partie de l'opinion publique lors d'un débat ou audience lors d'une émission culturelle.

C'est dire que le rôle joué par les participants au sein du processus d'innovation technologique est intimement lié à la *représentation* que ceux-ci se font de l'usager, à commencer par la définition qu'ils en adoptent. Cette définition implique évidemment aussi une définition des usages anticipés que l'utilisateur fera d'un objet technique, ainsi que de ses droits et ses devoirs en regard de l'utilisation de cet objet.

Ainsi, David Chaum définit l'utilisateur comme un citoyen, doté de libertés civiques — l'anonymat, par exemple — qu'il est en droit de protéger. Toute nouvelle manifestation technologique de la monnaie ne devrait pas modifier les paramètres fondamentaux de la vie civique de l'usager. Celui-ci est évidemment convaincu que les usagers eux-mêmes partagent cette opinion , comme le note LEVY (1994) :

> « *He says that if, after knowing that the possibility of private, digital-monetary transactions exists, people opt to spend their money with the same traceability as credit cards, he will accept the decision. But he doesn't think that will happen. His guess is that once people are aware of the issues, they will agree that traceable routes are the evil of all money.* »

De façon similaire, les industries se doivent de définir l'usager (habituellement en tant que consommateur) et ses utilisations anticipées de l'objet technique, quitte à devoir réévaluer leur position selon le succès de leur produit. Ce processus est cependant coûteux et les industries ont compris depuis longtemps que le couplage entre un produit et son public s'effectue d'autant mieux que l'on dispose du consommateur approprié : il s'agit alors de le prédisposer à désirer l'objet en question, quitte à en créer le besoin de toutes pièces si jamais celui-ci s'avérait inexistant, tâche dont s'acquittent les agences de marketing et de publicité. [2]

Pourtant, si chacun des intervenants se forge une représentation de l'usager et tente de prescrire les utilisations qu'il fera de l'objet technique, celui-ci se l'approprie, dévie des schèmes préétablis et crée des mécanismes d'utilisation qui lui sont propre, « Zapping » télévisuel, messageries roses sur Minitel, autant de manifestations du pouvoir de l'utilisateur à manier les objets techniques hors des étroits sentiers qui lui sont proposés.

Au-delà des manifestations de sa déviance, l'usager tente de faire valoir ses besoins par l'entremise de groupes de pression qui tentent eux aussi d'influencer le processus de design. Ainsi, au sein de la communauté cryptologique, des chercheurs se sont regroupés en des associations vouées à la défense des libertés civiles [3], qu'ils jugent les plus adéquatement protégées par l'utilisation non réglementée de la cryptographie. Les associations de consommateurs auront aussi probablement un rôle à jouer à l'égard de la représentation de l'usager, mais le fait demeure qu'il est difficile de donner voix à un être aussi élusif, et que la légitimité de ces portes-paroles reste à déterminer.

* * *

Au terme de ce mémoire, nous disposons d'une appréciation plus fine des motivations et des enjeux reliés au développement des produits de monnaie électronique. Le rôle des différentes contraintes techniques, de même que celui des différents groupes actifs au sein du processus de design, nous apparaît plus clairement, et l'on pourrait facilement croire que les fortes préoccupations sociales qui paraissent animer la communauté universitaire sont un gage que l'introduction des espèces numériques au sein de nos sociétés s'effectuera de façon réfléchie et démocratique.

Malheureusement, les traditions qui régissent le processus d'innovation technologique et le poids des intérêts commerciaux nous inclinent à croire que les impératifs économiques seront une fois de plus invoqués pour justifier la mise en place d'une in-

2. Le lecteur qui désire s'en convaincre consultera l'ouvrage de SMITH (1993), où est magistralement illustrée la manière par laquelle les grands fabricants américains d'automobiles se sont activement employés à la création de l'imagerie psychologique et sociale qui associe l'automobile à l'évasion et à la liberté individuelle, de façon à pouvoir écouler leur production massive.

3. Par exemple, l'*Electronic Frontier Foundation*, les *Cypherpunks*, et les *Computer Scientists for Social Responsability*.

frastructure technologique importante et peu flexible. Les formes qu'adoptera la monnaie électronique seront probablement largement déterminées de façon unilatérale par le processus du marché, et les usagers disposeront d'un « choix » entres plusieurs produits essentiellement similaires. L'implantation à grande échelle en Belgique d'un procédé de monnaie électronique, tel que relaté par THE ECONOMIST (1997), semble confirmer que les préoccupations de protection des libertés civiles qui motivent la communauté de recherche ne survivront pas à la logique du marché, même lorsque les pouvoirs publics sont impliqués. Les usagers semblent devoir demeurer confinés à exercer leur seul « pouvoir » de consommateur, plutôt que d'exercer une part plus active lors de la réalisation d'objets techniques avec lesquels ils sont appelés à interagir de façon intensive. Ainsi, notre relation à des objets inscrits au cœur de l'activité quotidienne tendra à être colorée du sentiment d'impuissance et de dépendance qui semble si souvent le nôtre face à la complexité de l'univers technologique qui nous entoure.

Références

ABE, M. et E. FUJISAKI (1996), « How to Date Blind Signatures », in *Advances in Cryptology — ASIACRYPT '96 Proceedings*, Springer-Verlag, pp. 244–251.

ALDERMAN, E. et C. KENNEDY (1995), *The Right to Privacy*, New York, NY : Alfred A. Knopf.

ANDERSON, R. J. (1994), « Liability and Computer Security: Nine Principles », in *Proceedings, European Symposium on Research in Computer Security — ESORICS '94*, Springer-Verlag, pp. 231–245.

ANDERSON, R. J. (1995), « Why Cryptosystems Fail », *Communications of the ACM 37*(11), pp. 32–40.

ANDERSON, R. J. (1996), « Security in Clinical Information Systems », British Medical Association.

ANDERSON, R. J. et S. J. BEZUIDENHOUT (1995), « Cryptographic Credit Control in Pre-Payment Metering Systems », in *Proceedings,1995 IEEE Computer Society Symposium on Research in Security and Privacy*, IEEE Computer Society Press, pp. 15–23.

ANDERSON, R. J. et S. J. BEZUIDENHOUT (1996), « On the Reliability of Electronic Payment Systems », *IEEE Transactions on Software Engineering 22*(5), pp. 294–301.

ANDERSON, R. J. et M. KUHN (1996), « Tamper Resistance — A Cautionary Note », in *Proceedings of the Second USENIX Workshop on Electronic Commerce*, USENIX Association, pp. 1–11.

BABBAGE, C. (1833), *Traité sur l'économie des machines et des manufactures*, Bruxelles : Louis Hauman et C^ie^ .

BACON, J. (1993), *Concurrent Systems*, New York, NY : Addison-Wesley Publishing Co.

BANQUE DES RÈGLEMENTS INTERNATIONAUX (1996), *Security of Electronic Money*, Bâle : Banque des Règlements Internationaux.

BAUMOL, W. J., A. S. BLINDER et W. S. SCARTH (1988), *Economics: Principles and Policy*, Toronto : Harcourt Brace Jovanovich.

BOLY, J.-P., A. BOSSELAERS, R. CRAMER, R. MICHELSEN, S. MJØLSNES, F. MULLER, T. PEDERSEN, B. PFITZMANN, P. DE ROOIJ, B. SCHOENMAKERS, M. SCHUNTER, L. VALLÉE et M. WAIDNER (1994), « The ESPRIT Project CAFE — High Security Digital Payment Systems », in *Third European Symposium on Research in Computer Security — ESORICS '94*, Springer-Verlag, pp. 217–230.

BOULLIER, D. (1994), « Construire le téléspectateur : Récepteur, consommateur ou citoyen ? », in *Médias et nouvelles technologies : Pour une socio-politique des usages*, Rennes : Éditions Apogée, pp. 63–74.

BRANDS, S. (1993), « An Efficient Off-Line Electronic Cash System Based On The Representation Problem », Technical Report CS-R9323, CWI, Amsterdam.

BRANDS, S. (1994a), « Off-Line Cash Transfer by Smart Cards », in *Proceedings, First Smart Card Research and Advanced Application Conference*, pp. 101–117.

BRANDS, S. (1994b), « Untraceable Off-Line Cash in Wallets with Observers », in *Advances in Cryptology — CRYPTO '93 Proceedings*, Springer-Verlag, pp. 302–318.

BRANDS, S. (1995), « Electronic Cash on the Internet », in *Proceedings, 1995 Symposium on Network and Distributed System Security*, IEEE Computer Society Press, pp. 25–39.

BRASSARD, G. (1992), *Cryptologie contemporaine*, Paris : Masson.

BRICKELL, E., P. GEMMELL et D. KRAVITZ (1995), « Trustee-Based Tracing Extensions to Anonymous Cash and the Making of Anonymous Change », in *Proceedings of the 6th Annual Symposium on Discrete Algorithms*, pp. 457–466.

CAMENISCH, J., U. M. MAURER et M. STADLER (1996), « Digital Payment Systems with Passive Anonymity-Revoking Trustees », in *Proceedings of the Fourth European Symposium on Research in Computer Security: ESORICS '96*, Springer-Verlag, pp. 33–43.

CAMENISCH, J., J.-M. PIVETEAU et M. STADLER (1994), « An Efficient Payment System Protecting Privacy », in *Third European Symposium on Research in Computer Security — ESORICS '94*, Springer-Verlag, pp. 207–215.

CAMENISCH, J., J.-M. PIVETEAU et M. STADLER (1996), « An Efficient Fair Payment System », in *Third ACM Conference on Computer and Communications Security*, ACM Press, pp. 88–94.

CHAUM, D. (1981), « Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms », *Communications of the ACM 24*(2), pp. 84–88.

CHAUM, D. (1983), « Blind Signatures for Untraceable Payments », in *Advances in Cryptology: Proceedings of CRYPTO 82*, Plenum Press, pp. 199–203.

CHAUM, D. (1984), « Blind Signature System », in *Advances in Cryptology: Proceedings of CRYPTO 83*, Plenum Press, p. 153.

CHAUM, D. (1985), « Security Without Identification: Transaction Systems to Make Big Brother Obsolete », *Communications of the ACM 28*(10), pp. 1030–1044.

CHAUM, D. (1988), « The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability », *Journal of Cryptology 1*, pp. 65–75.

CHAUM, D. et J.–H. EVERTSE (1987), « A Secure and Privacy-Protecting Protocol for Transmitting Personal Information Between Organizations », in *Advances in Cryptology — CRYPTO '86 Proceedings*, Springer-Verlag, pp. 118–167.

CHAUM, D., A. FIAT et M. NAOR (1988), « Untraceable Electronic Cash », in *Advances in Cryptology — CRYPTO '88 Proceedings*, Springer-Verlag, pp. 319–327.

CHAUM, D. et T. P. PEDERSEN (1992a), « Transferred Cash Grows in Size », in *Advances in Cryptology — EUROCRYPT '92 Proceedings*, Springer-Verlag, pp. 89–105.

CHAUM, D. et T. P. PEDERSEN (1992b), « Wallet Databases with Observers », in *Advances in Cryptology — CRYPTO '92 Proceedings*, Springer-Verlag, pp. 89–105.

COX, B. T. (1994), *Maintaining Privacy in Electronic Transactions*, Mémoire de maîtrise, Carnegie Mellon University.

CRAMER, R. J. et T. P. PEDERSEN (1994), « Improved Privacy in Wallets with Observers », in *Advances in Cryptology — EUROCRYPT '93 Proceedings*, Springer-Verlag, pp. 329–343.

DAVIDA, G., Y. FRANKEL, Y. TSIOUNIS et M. YUNG (1997), « Anonymity Control in E-Cash Systems », *Financial Cryptography '97 Proceedings* (à paraître).

DAVIES, G. (1994), *A History of Money: From Ancient Times to the Present Day*, Cardiff : University of Wales Press.

DAVIS, P. J. et R. HERSH (1981), *The Mathematical Experience*, Boston : Houghton Mifflin Company.

DEN BOER, B., D. CHAUM, E. VAN HEYST, S. MJØLNES et A. STEENBEEK (1990), « Efficient Off-line Electronic Checks », in *Advances in Cryptology — EUROCRYPT '89 Proceedings*, Springer-Verlag, pp. 294–301.

FAGIN, R., M. NAOR et P. WINKLER (1996), « Comparing Information Without Leaking It », *Communications of the ACM 39*(5), pp. 77–85.

FERGUSON, N. (1994), « Single Term Off-Line Coins », in *Advances in Cryptology — EUROCRYPT '93 Proceedings*, Springer-Verlag, pp. 318–328.

FIAT, A. et A. SHAMIR (1987), « How To Prove Yourself: Practical Solutions to Identification and Signature Problems », in *Advances in Cryptology — CRYPTO '86 Proceedings*, Springer-Verlag, pp. 186–194.

FRANKEL, Y., Y. TSIOUNIS et M. YUNG (1996), « "Indirect Discourse Proofs": Achieving Efficient Fair Off-Line E-Cash », in *Advances in Cryptology — ASIACRYPT '96 Proceedings*, Springer-Verlag, pp. 286–300.

FRANKLIN, M. et M. YUNG (1992), « Towards Provably Secure Efficient Electronic Cash », Technical Report TR CUCS-018-92, Columbia University.

GIEDION, S. (1948), *Mechanization Takes Command : A Contribution to Anonymous History*, Oxford : Oxford University Press.

GLASSMAN, S., M. MANASSE, M. ABADI et P. GAUTHIER (1995), « The Millicent Protocol for Inexpensive Electronic Commerce », in *Fourth International World Wide Web Conference Proceedings*, O'Reilly & Associates, pp. 603–618.

HAUSER, R., M. STEINER et M. WAIDNER (1996), « Micro-Payments Based on iKP », Technical Report RS 2791, IBM Research Division, Zürich.

HIRSCHFELD, R. (1993), « Making Electronic Refunds Safer », in *Advances in Cryptology — CRYPTO '92 Proceedings*, Springer-Verlag, pp. 106–112.

HOFFMAN, L. J. (édit.) (1995), *Building in Big Brother: The Cryptographic Policy Debate*, Berlin : Springer–Verlag.

JAKOBSSON, M. (1995a), « Blackmailing Using Undeniable Signatures », in *Advances in Cryptology — EUROCRYPT '94 Proceedings*, Springer-Verlag, pp. 425–427.

JAKOBSSON, M. (1995b), « Ripping Coins for a Fair Exchange », in *Advances in Cryptology — EUROCRYPT '95 Proceedings*, Springer-Verlag, pp. 220–230.

JAKOBSSON, M. et M. YUNG (1996), « Revokable and Versatile Electronic Money », in *3rd ACM Conference on Computer and Communications Security*, ACM Press, pp. 76–87.

KAHN, D. (1967), *The Codebreakers: The Story of Secret Writing*, New York, NY : Macmillan Publishing Co.

LANDAU, S. (1983), « Primes, Codes and the National Security Agency », *Notices of the American Mathematical Society 30*(1), pp. 7–10.

LANDAU, S. (1988), « Zero Knowledge and the Departement of Defense », *Notices of the American Mathematical Society 35*(1), pp. 5–12.

LAW, L., S. SABETT et J. SOLINAS (1996), « How to Make a Mint: The Cryptography of Anonymous Electronic Cash », Technical report, National Security Agency : Office of Information Security Research and Technology, Cryptology Division.

LENSTRA, A. (1996), « Factorization of RSA-130 Using the Number Field Sieve », Message publié sur le forum `sci.crypt.research`, 14 avril 1996.

LEVY, S. (1994), « E-money (That's What I Want) », *Wired 2*(12), pp. 174–179.

MARX, G. T. (1986), « The Iron Fist and the Velvet Glove: Totalitarian Potentials Within Democratic Structures », in *The Social Fabric: Dimensions and Issues*, Beverly Hills, CA : Sage Publications, pp. 135–161.

MENEZES, A. J., P. C. VAN OORSCHOT et S. A. VANSTONE (1997), *Handbook of Applied Cryptography*, Boca Raton, FL : CRC Press.

MICALI, S. (1992), « Fair Public-Key Cryptosystems », in *Advances in Cryptology — CRYPTO '92 Proceedings*, Springer-Verlag, pp. 113–138.

NEWTON, J. (1996), *Organised Plastic Counterfeiting*. Her Majesty's Stationery Office, ISBN 0-11-341128-6.

NYE, D. E. (1990), *Electrifying America: Social Meanings of a New Technology*, Cambridge, MA : MIT Press.

OFFICE OF TECHNOLOGY ASSESSMENT, U.S. CONGRESS (1995), *Information Technologies for Control of Money Laundering*, Washington, DC : Government Printing Office, OTA-ITC-630.

OKAMOTO, T. (1995), « An Efficient Divisible Electronic Cash Scheme », in *Advances in Cryptology — CRYPTO '95 Proceedings*, Springer-Verlag, pp. 438–451.

OKAMOTO, T. et T. ENG (1994), « Single-Term Divisible Electronic Coins », in *Advances in Cryptology — EUROCRYPT '94 Proceedings*, Springer-Verlag, pp. 311–323.

OKAMOTO, T. et K. OHTA (1990), « Disposable Zero-Knowledge Authentications and their Applications to Untraceable Electronic Cash », in *Advances in Cryptology — CRYPTO '89 Proceedings*, Springer-Verlag, pp. 481–497.

OKAMOTO, T. et K. OHTA (1992), « Universal Electronic Cash », in *Advances in Cryptology — CRYPTO '91 Proceedings*, Springer-Verlag, pp. 324–337.

ORWELL, G. (1949), *Nineteen Eighty-four*, New York, NY : Harcourt, Brace and Company, Inc.

PASCAL (1654), « Lettre à Fermat, 29 juillet 1654 », in *Œuvres Complètes*, Paris : Bibliothèque de la Pléiade, pp. 77–83.

PEDERSEN, T. P. (1995), « Electronic Payments of Small Amounts », Technical Report DAIMI PB-495, Århus Universitet.

PFITZMANN, A., B. PFITZMANN, M. SCHUNTER et M. WAIDNER (1996), « Mobile User Devices and Security Modules: Design for Trustworthiness », Technical Report RZ 2784, IBM Research Division, Zürich.

PFITZMANN, A. et M. WAIDNER (1986), « Networks Without User Observability — design options », in *Advances in Cryptology — EUROCRYPT '85 Proceedings*, Springer-Verlag, pp. 245–253.

PFITZMANN, B. et M. WAIDNER (1995), « Strong Loss Tolerance for Untraceable Electronic Coin Systems », Technical Report ISSN 0941–3014, Institut für Informatik, Universität Hildesheim.

PFITZMANN, B. et M. WAIDNER (1996), « Properties of Payment Systems: General Definition, Sketch and Classification », Technical Report RZ 2823, IBM Research Division, Zürich.

PROULX, S. (1994), « Les Différentes problématiques de l'usage et de l'usager », in *Médias et nouvelles technologies : Pour une socio-politique des usages*, Rennes : Éditions Apogée, pp. 149–159.

RIGAUX, F. (1990), *La Protection de la vie privée et des autres biens de la personnalité*, Bruxelles : Établissements Émile Bruylant, Paris : Librairie Générale de Droit et de Jurisprudence.

RIVEST, R. L. (1990), « Cryptography », in *Handbook of Theoretical Computer Science (Volume A: Algorithms and Complexity)* : Elsevier and MIT Press, Chapter 13, pp. 717–755.

RIVEST, R. L. et A. SHAMIR (1996), « PayWord and MicroMint: Two Simple Micropayment Schemes », *CryptoBytes 3*(1), pp. 7–11.

RIVEST, R. L., A. SHAMIR et L. M. ADLEMAN (1978), « A Method for Obtaining Digital Signatures and Public-Key Cryptosystems », *Communications of the ACM 21*(2), pp. 120–126.

SIMMONS, G. J. (édit.) (1992), *Contemporary Cryptology: The Science of Information Integrity*, Piscataway, NJ : IEEE Press.

SMITH, T. (1993), *Making the Modern : Industry, Art, and Design in America*, Chicago, IL : The University of Chicago Press.

STADLER, M. (1996), *Cryptographic Protocols for Revocable Privacy*, Thèse de doctorat, Swiss Federal Institute of Technology (Zürich).

STADLER, M., J.-M. PIVETEAU et J. CAMENISCH (1995), « Fair Blind Signatures », in *Advances in Cryptology — EUROCRYPT '95 Proceedings*, Springer-Verlag, pp. 209–219.

STINSON, D. R. (1995), *Cryptography : Theory and Practice*, Boca Raton, FL : CRC Press.

THE ECONOMIST (1997), « Electronic Money : Chipper, for now », *The Economist*, April 26th, p. 72–77.

VAN ANTWERPEN, H. (1990), *Off-Line Electronic Cash*, Mémoire de maîtrise, Eindhoven University of Technology.

VEDEL, T. (1994), « Sociologie des innovations technologiques et usagers : Introduction à une socio-politique des usages », in *Médias et nouvelles technologies : Pour une socio-politique des usages*, Rennes : Éditions Apogée, pp. 13–34.

VITALIS, A. (1988), *Informatique, pouvoir et libertés*, Paris : Economica.

VITALIS, A. (1994), « La Part de citoyenneté dans les usages », in *Médias et nouvelles technologies : Pour une socio-politique des usages*, Rennes : Éditions Apogée, pp. 35–43.

VON SOLMS, S. et D. NACCACHE (1992), « On Blind Signatures and Perfect Crimes », *Computers and Security 11*(6), pp. 581–583.

WAIDNER, M. et B. PFITZMANN (1990), « Loss-Tolerance for Electronic Wallets », in *Proceedings of the 20th International Symposium on Fault-Tolerant Computing*, pp. 140–147.

WINNER, L. (1977), *Autonomous Technology: Technics-Out-of-Control as a Theme in Political Thought*, Cambridge, MA : MIT Press.

WINNER, L. (1986), *The Whale and the Reactor: A Search for Limits in an Age of High Technology*, Chicago, IL : The University of Chicago Press.

ZUBOFF, S. (1988), *In the Age of the Smart Machine : The Future of Work and Power*, New York : Basic Books.