Université de
Montréal

Étude comparative des moyens de paiement

Par

ABDOULAYE
HAMADOU

Département d'**I**nformatique et de **R**echerche
Opérationnelle

Faculté des arts et sciences

Mémoire présenté à la Faculté des études supérieures
et
postdoctorales
En vue de l'obtention du grade de maître ès (M.sc.)
en informatique

Avril, 2015

Résumé

L'époque où il n'existait qu'un choix restreint de modes de paiement est à présent révolue. En effet, de l'apparition de la monnaie fiduciaire aux trente glorieuses, ils n'avaient que très peu évolué. Or, depuis quelques décennies, nous assistons à l'apparition de nombreux moyens de paiement, tous plus différents les uns des autres. Notre présente étude a non seulement pour objectif d'en confronter les principaux en vue d'identifier le plus adéquat face à une situation donnée, mais aussi et surtout de discuter de l'**anonymat** que ces derniers procurent ou non.

Pour ce faire, nous avons d'abord présenté chacun de ces moyens tout en en définissant les fonctionnements et les technologies. Par la suite, une comparaison par l'entremise d'une analyse indépendante a été réalisée sur la base d'éléments précis tels que la **protection de la vie privée** ou encore les **propriétés ACID**. Des critères comme la **confiance des utilisateurs (sécurité)** et **les attentes qu'ont les institutions financières** vis-à-vis de ces derniers ont aussi été considérés. Et enfin, trois méthodes de paiement qui sont en réalité des approches-solutions pour pallier aux problèmes liés à l'anonymat que présentent certains principaux moyens de paiement connus, ont été présentées à leur tour. Ainsi, le premier système de paiement proposé est axé sur les **comptes bancaires anonymes**, tandis que le second est, lui inspiré du système des **jetons**; Si bien qu'une combinaison de ces deux approches a conduit à une troisième, afin d'en regrouper les avantages.

Mots-clés : ACID, anonymat, cryptographie, paiement, sécurité.

Abstract

The time we used to only have one option of method payment is now long gone. As a matter of fact, from the apparition of currency until the « thirty glorious years », nothing new in this field appeared. It is true, in the last decades we are witnessing the birth of many of means of payment, all more different from each other. This study, therefore, aims to confront the principal means of payment but also to discuss about the question of anonymity that may come with it.

To do so, will be presented each of every means of payment separately while describing all their functions and technologies. Then, a comparison will be presented through an independent analysis that was carried out on specific elements such as: the **protection of private life** and **properties ACID**. Other elements like **users'trust (security)** and **expectations from the financial institutions** will also be considered. Finally, three problems solving in relation to the anonymity of the current means payment known today, will constitute the last section. The first solution focuses on the **anonymous bank accounts**, the second is inspired from the **token system**; The last, but not least, combines the two first systems in order to combine the advantages.

keys-word : ACID, Anonymity, cryptography, payment, security.

Table des matières

Liste des tableaux :

Liste des figures :

Liste des sigles et abréviations :

ACID : Atomicité Cohérence Isolation Durabilité

STM : Société des Transports de Montréal

BC : Banque du Canada

TPE : Terminal de Paiement Électronique

UIT : Union Internationale des Télécommunications

MRC : Monnaie Royale du Canada

GRC : Gendarmerie Royale du Canada

ACP : Association Canadienne de Paiements

ABC: Association des Banquiers Canadiens

NIP : Numéro d'Identification Personnel

RSA: Rivets, Shamir et Adleman

MIT: Massachusetts Institute of Technology

CAM : Code d'authentification des Messages

EEPROM : Electrically-Erasable Programmable Read-Only Memory ou mémoire morte effaçable électriquement et programmable

RFID : Radio Frequency Identification Devices

DCSSI : Direction Centrale de la Sécurisation des Systèmes d'Informations

PVC : Polychlorure de vinyle

ISO : International Standard Organisation /Organisation Internationale de normalisation

ANSI: American National Standards Institute

EMV: Eurocard Mastercard Visas

VISA : Visa International Service Association

DAB : Distributeurs Automatique de Billets

SDA : Static Authentification Data / l'Authentification Statique des Données

DDA : Dynamic Data Authentification/ Authentification Dynamique des Données

CDA : Combined Data Authentification / Authentification Combinées des Données

CA : Cryptogramme d'Application

UCC : Union des Consommateurs du Can deux premières phases ada

ABC : Association des Banquiers Canadiens

AC : Autorité de certification

AVAB : Autorité de vérification d'autorisation bancaire

AA : Autorité d'anonymisation

SSL : Secure Socket Layer

TLS : Transport Layer Security

À ma grand-mère,

à mes parents, à mes frères et sœurs

je dédie ce modeste travail

preuve de mon amour car, rien n'est

plus difficile que d'avouer son amour.

Je vous aime !!!

Remerciements

Je tiens tout d'abord à remercier M. Louis SALVAIL, mon directeur de recherche, pour sa patience, son soutien, ses précieux conseils ainsi que pour l'aide apportée tout au long de la réalisation de ce mémoire.

Je tiens ensuite à remercier mes parents, sans qui je n'en serais pas là aujourd'hui. Merci pour le soutien financier, moral et les encouragements dont vous avez fait preuve tout au long de ma vie.

Je souhaite aussi remercier Aboubacar SIDIKI TONE, Tanobla Carine BADOU, Naomie LEWIS, Muriel HUE-BI, Warren MVONDO. Merci pour vos conseils et vos remarques pertinentes qui ont aidé à l'élaboration de ce travail.

Enfin, merci à tous ceux qui, de près ou de loin, ont contribué à l'accomplissement de ce mémoire.

Introduction

Big Brother est partout. En effet, comme nous l'a démontré l'affaire Snowden, nos faits et gestes sont beaucoup plus observés qu'il y a quelques décennies pour ″des raisons de sécurité nationale″. Aujourd'hui personne ne peut passer inaperçu, aucune vie ne reste véritablement privée. Malheureusement, les moyens de paiement dont nous usons contribuent d'une certaine manière à cette surveillance. Naturellement nous aimerons tous avoir un moyen de paiement sûr, anonyme et qui protègerait notre vie privée.

Qui peut se targuer de n'avoir jamais entendu cette phrase au moins une fois : Comment désirez-vous payez? Par chèque, comptant, carte de débit, carte de crédit...

Alors, en être au fait nous aiderait à choisir le plus adéquat selon les circonstances. La pertinence de cette problématique est d'autant plus intéressante que les objectifs des utilisateurs varient selon les achats et les lieux où ils sont effectués.

C'est alors qu'une documentation traitant des moyens de paiement et des technologies afférentes couplée à une analyse personnelle permettront de répondre à cette question à travers une série d'interrogations inhérentes au sujet à savoir : Quel est le moyen de paiement le plus sécuritaire? Quel est celui qui garantit un parfait anonymat? Quel est celui qui protège le mieux la vie privée? Lequel confère-t-il le plus d'avantages?

Comme son intitulé l'indique : "Étude Comparative des moyens de paiement", ce mémoire tend à comparer les principaux moyens de paiement pour mettre en exergue celui qui se rapproche le plus des volontés des utilisateurs et si nécessaire en améliorer certains aspects.

Pour ce faire, il s'articulera autour de cinq chapitres. Ainsi, après le chapitre 1 qui exposera les définitions et introduira les deux principaux moyens de paiement dits « traditionnels » que sont le chèque et la monnaie fiduciaire ; Le chapitre 2 traitera des méthodes et outils cryptographiques utilisés pour les moyens de paiement électroniques. Quant au chapitre 3, il discutera dans un premier temps de DigiCash, le premier mode de paiement électronique proposant l'anonymat, puis dans un second temps de bitcoin, qui est une monnaie électronique décentralisée.

Le chapitre 4 sera celui des cartes à puce et il s'attardera sur les cartes de crédit et de débit qui sont les plus courantes.

Enfin, dans le chapitre 5 nous développerons deux moyens de paiement qui, en dépit de la conjecture actuelle, pourraient être réalisés sur la base des systèmes déjà existants. De fait, d'un côté l'anonymisation des comptes bancaires à travers l'utilisation des pseudonymes et des tiers de confiance tout en conservant le système utilisé par les cartes de débit sera présentée, et de l'autre, nous évoquerons un second système inspiré des cartes « opus » de la Société des Transports de Montréal (STM), qui sera axé sur des jetons rechargeables. Dans la foulée, un troisième système fusionnant certains bienfaits des deux qui précèdent, afin d'en amoindrir les désavantages sera finalement proposé.

Chapitre 1. Définitions et moyens de paiement traditionnels.

Il est communément admis qu'une acquisition tout comme une demande de service requiert l'utilisation d'un moyen de paiement. Un moyen de paiement est défini comme étant « un support de transactions courantes dont disposent les particuliers et les entreprises pour solder le prix d'un bien ou d'un service » [1].

Le long du premier chapitre, les divers moyens de paiement et leurs concepts de base, ainsi que les acteurs et institutions qui y sont associées seront examinés. Il traitera également du fonctionnement général des moyens de paiement présentés. Enfin, la monnaie fiduciaire et le chèque bancaire seront proposés en exemple de paiements dits « traditionnels ».

1.1. Définitions.

Un ***achat*** est défini comme étant le processus d'acquisition d'un bien ou d'un service en contrepartie d'un paiement fait par un client. Nous pouvons dès à présent définir le ***client*** comme une ″personne qui reçoit d'une entreprise, contre paiement, des fournitures commerciales ou des services″ qui lui sont fourni par un vendeur [1.1]. Tandis que le ***vendeur*** sera lui ″une personne physique ou morale qui procède à une vente″ [1.1] ; tout en sachant qu'une ***vente*** est la cession d'un bien ou d'un service en contrepartie d'une rémunération.

À la lumière des définitions précédentes et pour les besoins du présent mémoire, il est utile de signifier que les clients et les vendeurs constituent des sous-ensembles d'une même entité: les ***utilisateurs.*** Aussi, regrouperons-nous, sous l'expression ***institutions financières***, les entités économiques qui s'occupent du commerce de l'argent**.** L'article 34 de la législation française les régissant précise qu'il s'agit des banques, des organismes d'épargne postale ou de crédit, des sociétés de bourse ou d'assurances, ou toute autre institution déclarée telle par le département auprès du conseil d'État [2] .

Toutefois, nous avons plusieurs types de commerces en rapport aux différents types de monnaie que sont les monnaies électronique, fiduciaire et scripturale. La Banque du Canada (BC), dans son glossaire, définit la ***monnaie électronique*** comme un instrument de paiement dont la valeur monétaire est stockée sur un support électronique [1.2].

D'où les espèces (billets de banque et pièces) produites par l'institut d'émission et ayant cours légal sur un territoire représentent la ***monnaie fiduciaire*** [3] . La ***monnaie scripturale*** est, quant à elle, composée de tous les moyens de paiement qui impliquent la présence d'une écriture sur un compte [1]. Cependant, l'utilisation de l'une ou l'autre de ces monnaies nécessite à un moment ou à un autre l'intervention d'une banque, tant et si bien qu'il est primordial de savoir ce qu'est une banque. La ***banque*** est un «établissement financier qui reçoit des fonds du public et les emploie pour effectuer des opérations de crédit et des opérations financières. Il est chargé de l'offre et de la gestion des moyens de paiement» [1.1], au nombre desquels on peut ajouter la carte bancaire. En effet, la ***carte bancaire*** est, selon la Fédération Bancaire Française, un moyen de paiement prenant la forme d'une carte émise par un établissement de crédit. Elle permet à son titulaire, conformément au contrat qui le lie à sa banque, d'effectuer des paiements et/ou des retraits d'argent; Des services connexes peuvent y être associés tels que les assurances et les assistances [1.3] . Il faudrait toutefois noté qu'il existe deux principaux types de cartes bancaires à savoir la carte de crédit et la carte de débit.

C'est ainsi que, cette même fédération définit la ***carte de crédit*** comme étant une carte de paiement permettant à son titulaire de régler des achats et/ou d'effectuer des retraits d'argent au moyen d'un crédit préalablement et contractuellement déterminé. À contrario, la ***carte de débit*** permet à son titulaire de régler des achats et/ou d'effectuer des retraits d'argent, les montants sont généralement débités au jour le jour, et ce à partir d'un compte chèque [1.3] . Ces deux types de cartes sont le plus souvent liés à un compte bancaire.

L'utilité d'expliquer ce qu'est un ***compte bancaire*** s'impose donc. En accord avec le dictionnaire en ligne becompta.be, c'est « un compte attribué à chaque client pour un ou plusieurs produits financiers. Il permet de tracer les entrées, sorties et soldes d'argent de ce client pour ce ou ces produits (compte courant, compte d'épargne, compte de titres, compte de prêt ...)» [1.4] . Il faut tout de même noter que, ce traçage auquel fait allusion le dictionnaire en ligne becompta.be est rendu possible par l'utilisation des moyens de paiement à l'exemple du chèque.

En effet, de par sa définition, le ***chèque*** illustre ce propos, car étant un ordre de paiement à travers lequel une personne appelée « tireur », demande à une banque (ou à un organisme autorisé par la loi) appelée « tirée », de payer une certaine somme d'argent à une tierce personne appelée « porteur » [4] . Ainsi, le chèque permet de transporter des unités monétaires sous forme papier par opposition au ***porte-monnaie électronique*** qui est un système plus récent permettant le transport des unités monétaires pré-chargées mais non réservées à l'achat d'un unique type de produits. Le terme porte-monnaie électronique est couramment utilisé pour désigner un système portatif où des unités électroniques de paiement sont stockées dans une mémoire interne, le plus souvent la carte à puce. Son but est d'effectuer des transactions de petits montants qui, autrement, seraient trop onéreuses, et ce, le plus souvent au travers d'un terminal de paiement électronique [5] . Le ***Terminal de Paiement Électronique (TPE)*** est un équipement qui, connecté aux services spécialisés de la banque, permet à un vendeur d'accepter et de traiter les paiements par cartes bancaires. Cet appareil peut être relié directement à une caisse enregistreuse afin de faciliter une ***transaction informatique*** [1.3] qui est une séquence d'opérations qui conduit à un état final cohérent et valide [6] .

Ainsi, les transactions informatiques doivent idéalement répondre aux propriétés ***ACID*** représentant l'acronyme pour les termes **Atomicité**, **Cohérence**, **Isolation** et **Durabilité** [6] que nous verrons plus en détails dans les pages suivantes. La ***cryptographie***, qui est l'étude des techniques servant à protéger le contenu des messages et à en assurer l'authenticité [7] , permet de sécuriser ces transactions en utilisant le chiffrement.

En effet, le chiffrement est une méthode de cryptage permettant à plusieurs interlocuteurs d'échanger des informations en ayant l'assurance qu'une tierce personne, même si elle les intercepte, n'ait accès à leur contenu [7] .

Il permet de contrer la ***double-dépense*** qui est l'utilisation avec succès d'une ou de plusieurs versions dupliquées d'une même monnaie électronique [1.5].

1.2. Caractéristiques des moyens de paiement.

Les moyens de paiement se doivent de satisfaire à des exigences. Certaines sont communes à tous et d'autres sont exclusivement requises pour les paiements électroniques. Ce sont ces différentes propriétés qui serviront d'éléments d'analyse par la suite.

1.2.1. Propriétés communes à tous les moyens de paiement.

Les propriétés idéales pour satisfaire les utilisateurs que les moyens de paiement doivent respecter sont en autres la confiance, le respect de la vie privée, l'anonymat et la non-traçabilité.

Effectivement, un moyen de paiement doit être caractérisé par la confiance qu'il inspire à ses utilisateurs. Pour cela, il doit pouvoir garantir une certaine sécurité, une authenticité, une facilité d'utilisation et une certitude de paiement. Mais ces acquis vont de pair avec la notion de respect de la vie privée. En effet, les utilisateurs d'un moyen de paiement doivent avoir la garantie que les informations fournies sont protégées. De ce fait, comme les recommandations X.800[1] le font remarquer « il est le droit des personnes de contrôler ou d'agir sur des informations les concernant, pouvant être collectées et stockées et également sur les personnes par lesquelles et auxquelles elles peuvent être divulguées »; [8] Car, non seulement la notion d'anonymat est très importante pour les utilisateurs, mais la non-traçabilité l'est d'autant plus. Il est significatif de préciser que l'**anonymat** est le fait qu'on ne puisse pas identifier un individu au travers du moyen de paiement utilisé et que la **non-traçabilité** quant à elle permet d'éviter toute corrélation entre le moyen de paiement, sa provenance ainsi que sa destination [9]. Cette dernière est de ce fait très importante, dans la mesure où elle renforce la notion d'anonymat.

[1] Recommandations de l'Union Internationale des Télécommunications (UIT) sur l'architecture de sécurité pour l'interconnexion en système ouvert d'application CCITT

1.2.2. Propriétés ACID désirées pour les moyens de paiement électroniques.

Toute transaction informatique se doit, dans l'idéal, de respecter les propriétés ACID. Les moyens de paiement électroniques, qui fonctionnent de la même manière, ne devraient donc pas déroger à ce principe [6] . Les propriétés requises que sont l'**atomicité**, de la **cohérence**, de l'**isolation** et de la **durabilité** seront présentées ci-après.

D'abord, une transaction est dite « **atomique** », lorsqu'elle s'effectue dans sa totalité ou pas du tout [6, 10, 11]. En cas de non-exécution totale, ses données doivent être remises à leur état initial. L'atomicité doit être garantie lors d'incidents techniques ou de catastrophes naturelles [6, 11].

Ensuite, il se dit d'une transaction qu'elle est « **cohérente** », lorsqu'elle passe d'un état initial T1 à un état final T2, tous deux valides, et que toutes les modifications au niveau de la base de données sont consistantes [6, 11].

Concernant l'**isolation**, Serge Miranda affirme que « si exécutée au même moment que d'autres, elle se produit de la même manière que si elle était seule, une transaction est alors considérée isolée » [6, 11].

Enfin, une transaction est **durable** lorsqu'après son exécution, le résultat final est conservé de façon permanente dans une base de données [6, 11, 12]. Cette propriété ne peut être garantie en cas d'incidents majeurs ou de catastrophes naturelles.

1.2.3. Attentes des institutions financières.

Les institutions financières attendent des moyens de paiement qu'ils soient sûrs, pratiques et qu'ils procurent des avantages commerciaux mesurables en plus d'avoir la confiance des utilisateurs [13]. Outre cela, ces institutions désirent des moyens de paiement contrôlables par leurs soins (carte bancaire contrôlée par les banques émettrices) ou par ceux d'un organisme tiers (monnaie fiduciaire contrôlée, au Canada par exemple, par la banque du Canada). En effet, si un moyen de paiement se veut prospère et durable il doit remplir ces critères si chers aux institutions financières et parfois même aux gouvernements. Néanmoins, comme nous le verrons un peu plus loin, certains moyens de paiement ont pour objectif principal de se défaire du contrôle des institutions financières et des gouvernements. Mais bien avant cela, évoquons leur fonctionnement général.

1.2. Fonctionnement global des moyens de paiement.

En règle générale, tous les moyens de paiement présentent le même squelette de fonctionnement.

La figure 1.1., issue du rapport de l'organisation des consommateurs canadiens le démontre bien.

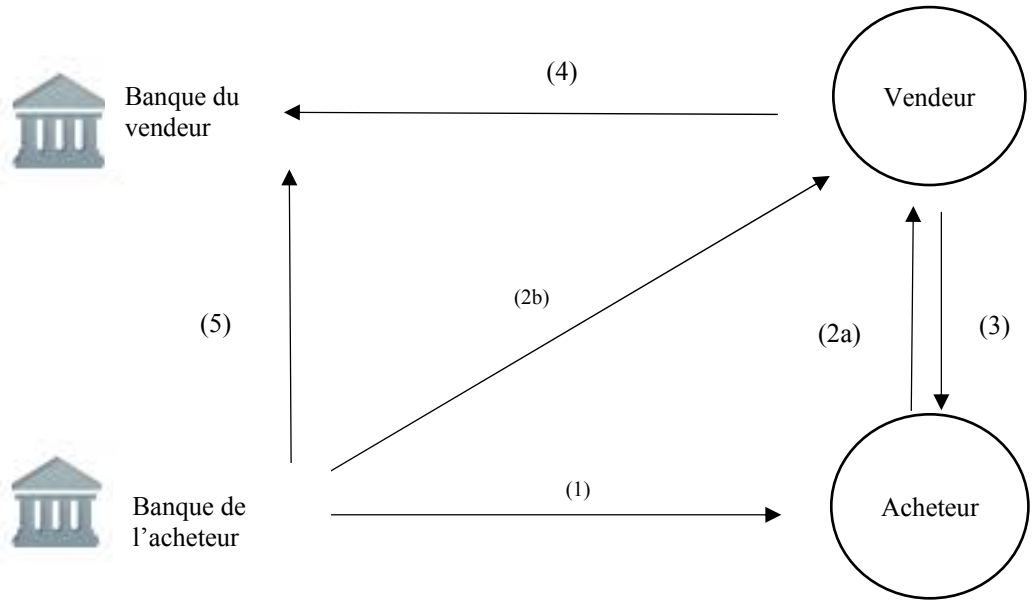

Figure 1.1. Fonctionnement global des moyens de paiement [14].

On comprend donc, grâce à la figure 1.1., que l'acheteur d'un bien ou d'un service commence par se procurer un moyen de paiement auprès de sa banque (1) (carte de crédit, argent fiduciaire, chèque bancaire…) qu'il peut utiliser (2a) pour régler le vendeur. Cependant, le choix lui est laissé de payer directement, par l'entremise de sa banque, grâce aux virements bancaires (2b). Évidemment en contrepartie, celui-ci remet à l'acheteur le bien ou le service auquel il a droit (3) conduisant ainsi le vendeur à déposer le moyen de paiement reçu à sa banque (4) (cette opération est uniquement nécessaire pour l'argent fiduciaire et le chèque bancaire). Dès lors, un flux national d'informations est partagé entre les banques de sorte que le compte de l'acheteur est débité pour créditer celui du vendeur (5) (ceci n'est valable que pour les opérations électroniques).

1.4. Menaces.

Regroupées en quatre catégories selon la classification des recommandations X.800 [Annexe A], les menaces peuvent être accidentelles, intentionnelles, passives ou actives [8]. Lorsqu'une menace plane sur un système (ici un moyen de paiement) et qu'elle n'est pas volontaire, on dit qu'elle est **accidentelle**.

Une défaillance dans un système, des bévues transactionnelles ou des bogues dans le logiciel sont des exemples de menaces accidentelles.

Le faux-monnayage est une illustration concrète de menace **intentionnelle**, qui par opposition à la précédente, nécessite une volonté d'altération (préméditation).

Par contre une menace **passive** n'altère ni les informations contenues dans le système, ni son fonctionnement intrinsèque, encore moins son état. L'observation des informations transmises par une ligne de communication à l'aide de branchements clandestins, en est un bon exemple. Contrastant avec cette dernière, une menace **active** entraine la modification de l'état ou du fonctionnement d'un système ainsi que l'altération des informations qu'il contient. La modification des tables de routages d'un système semble en être la parfaite illustration.

1.5. Moyens de paiement traditionnels.

À l'heure de la numérisation, la monnaie fiduciaire et le chèque sont devenus des moyens de paiement dits « traditionnels ». Dans cette sous-section, sous la base de certains critères nous les analyserons.

1.5.1. Monnaie fiduciaire.

La monnaie fiduciaire, grâce à sa simplicité d'utilisation, est l'un moyen de paiement privilégié des consommateurs. Elle est émise et distribuée par les banques centrales nationales pour ce qui est des billets de banque et les trésors publics concernant les pièces. Au Canada par exemple, ce sont la Banque du Canada[2] et la Monnaie Royale du Canada[3] qui ont le monopole de la fabrication et de la mise en circulation [1.6, 15].

Partant de ces entrefaites, une analyse de ce moyen de paiement est requise.

[2] http://www.banqueducanada.ca/
[3] www.mint.ca

Ainsi, pour acquérir la **confiance des utilisateurs**, la lutte contre le faux-monnayage doit être le principal souci des États et des organismes chargés de la conception et de la mise en circulation de l'argent liquide[4]. En effet, ces derniers redoublent d'ingéniosité pour combattre la contrefaçon.

Par exemple, depuis 2011 dans le cadre de l'intensification de sa lutte contre le faux-monnayage, la BC émet des billets en polymère dotés de nouveaux éléments de sécurité difficiles à contrefaire et facile à vérifier comme nous le montre la figure 1.2. suivante. [Annexe B] [16, 17]. La MRC, quant à elle depuis 2012, utilise une technique brevetée pour concevoir les pièces de un et de deux dollars (01 et 02 CAD), par blocage multicolore sur acier [1.7]. C'est une technique consistant à plaquer plusieurs couches successives de métaux (cuivre, nickel et laiton) sur le support en acier. De plus, au revers des pièces (du côté pile), une marque micro-gravée au laser et une image virtuelle sont ajoutées alors qu'un lettrage sur tranche est rajouté pour uniquement les pièces de deux dollars [1.7, 1.8]. Toujours dans le but de lutter contre la fraude, la loi canadienne concernant la répression contre le faux-monnayage dans son article 449 de la partie 7 sur les infractions relatives à la monnaie stipule qu'« est coupable d'un acte criminel et passible d'un emprisonnement maximal de quatorze ans quiconque fabrique ou commence à fabriquer de la monnaie contrefaite ». L'article 450 poursuit avec les avertissements en ces termes: « quiconque, sans justification ou excuse légitime, dont la preuve lui incombe, selon le cas :

a) achète, reçoit ou offre d'acheter ou de recevoir ;

b) a en sa garde ou possession ;

c) introduit au Canada, de la monnaie contrefaite, est coupable d'un acte criminel et est passible d'un emprisonnement maximal de quatorze ans » [1.9].

En outre, la monnaie fiduciaire en empêchant la collecte d'informations ayant trait à la **vie privée** en assure la protection. Elle préserve notamment les historiques d'achats, les fréquences des dépenses et les lieux où ont été effectuées les dépenses [18].

De plus, elle peut être considérée comme assurant l'**anonymat** à ses utilisateurs car ne contenant pas d'informations pouvant permettre leur identification ; Sans compter le fait qu'elle procure cette **non-traçabilité** qui maintient l'anonymat.

[4] Monnaie fiduciaire.

En effet, le commerçant n'est pas capable d'identifier la provenance de la monnaie qui lui est remise; Rien ne ressemble plus à un billet de dix dollars qu'un autre billet de dix dollars [18, 19].

Par ailleurs, la monnaie fiduciaire est **divisible**. Effectivement, pour un certain montant, il est possible d'obtenir la même valeur en coupures ou en pièces de valeurs inférieures [20]. Par exemple, un billet de vingt dollars canadiens peut être divisé en quatre billets de cinq dollars (05 CAD), qui peuvent à leur tour être échangés pour des pièces de valeurs moins importantes pour un montant final équivalent au montant initial de vingt dollars (20 CAD).

En plus de tout ce qui précède, la monnaie fiduciaire répond également à certains **critères réclamés par les institutions financières**. Il s'agit entre autre de la confiance qu'ont envers elle les utilisateurs, de la rapidité et de l'exactitude d'exécution lors des transactions. Il s'agit aussi de la sécurité relative aux fraudes qu'elle confère et surtout des avantages commerciaux qu'elle leur procure [1, 15] dans la mesure où le coût de fabrication de la monnaie fiduciaire est supporté par l'État [15].

Cependant, malgré ses atouts, la monnaie fiduciaire a des faiblesses. Elle doit faire face entre autre à des **menaces accidentelles**, par exemple le remboursement d'une monnaie supérieure à celle qui devrait l'être lors d'un achat. Ces **menaces** peuvent aussi être de nature **intentionnelle** et **active** comme le faux monnayage ou encore les braquages de banque [21].

Au vu des mentions précédentes, nous pouvons dire que la monnaie fiduciaire a de nombreux avantages. En effet, en plus d'être le symbole même de l'anonymat, l'union des consommateurs du Québec recense comme exemple d'avantages le fait qu'elle soit acceptée partout pour diverses transactions et qu'elle soit simple d'utilisation et rapide lors des paiements. En plus, elle facilite la tenue du budget en freinant les achats impulsifs et limite les erreurs dues à des tiers.

En revanche selon cette même union, elle présente certains inconvénients au nombre desquels le fait qu'elle puisse être relativement incommodante lors des achats de fort montant ou encore qu'elle limite les possibilités d'achats à distance. Lorsqu'elle est perdue ou volée, elle ne peut être récupérée. Aussi, l'utilisateur supporte seul les pertes liées à la possession d'une fausse monnaie [14, 18].

Figure 1.2. Éléments distinctifs d'un billet en polymère de vingt dollars canadiens [1.10].

1.5.2. Chèque.

Contrairement à la monnaie fiduciaire, le chèque est émis par la banque du tireur [4] . Lors d'un paiement par chèque, le tireur se doit de le remplir, conformément à la loi, en y indiquant les mentions obligatoires comme la figure l'indique 1.3. avant de le remettre au porteur [22,23]. Ce dernier pourra entrer en possession de son dû en présentant le chèque et une pièce d'identité à sa banque [4] . Néanmoins, cette simplicité a un coût pour les utilisateurs et exige des institutions émettrices une forme et des éléments constitutifs spécifiques [24].

Le chèque sera lui aussi analysé, et ce sur les mêmes critères que la monnaie fiduciaire.

C'est ainsi que, nous dirons que la **confiance des utilisateurs** doit être assurée par l'intégrité du chèque. Dans cette optique, les institutions financières doivent donc la garantir et ce e se conformant à certaines lois et directives [5, 24].

Au Canada par exemple, depuis 1992 l'Association Canadienne de Paiements[5] (ACP) publie une circulaire sur les formats d'impression des chèques visant à les rendre simples d'utilisation et sûrs. Hormis cela, chaque institution financière est libre de rajouter d'autres caractéristiques pour renforcer la sécurité de ses chèques [25].

[5] https://www.cdnpay.ca/imis15/fra/Home/fra/Home.aspx?languageId=1

Si ces méthodes permettent de prévenir la conception frauduleuse de chèques, elles ne sont malheureusement pas efficaces contre la falsification (imitation de signatures, changement du montant inscrit par le tireur sur le véritable chèque). De ce fait, pour lutter contre ce phénomène l'Association des Banquiers Canadiens[6] (ABC) conseille entre autres :

- de garder les chèques en lieux sûrs;
- de détruire les chèques restants lors de la clôture d'un compte bancaire et;
- de prêter attention aux relevés bancaires mensuels [26].

Cependant, le chèque ne garantit aucunement la **protection de la vie privée**. En effet, après son émission, il n'est plus possible d'effectuer quelque contrôle que ce soit, ni sur les informations qu'il contient ni sur l'utilisation qui en sera faite par le récipiendaire. L'émetteur du chèque est tout de même assuré d'une certaine protection et ce vis-à-vis des banques (ou autres institutions privées) puisqu'au Canada par exemple, elles sont soumises aux lois canadiennes relatives à la protection des renseignements personnels [1.13]. Si le tireur se trouve au Québec, il est de plus protégé par la loi québécoise sur la protection des renseignements personnels dans le secteur privé [26].

En outre, le chèque ne procure aucunement l'**anonymat**. Ceci est dû au fait que le tireur est dans l'obligation de mentionner ses informations civiles (noms, prénoms, adresse etc.) et ce, en plus des informations bancaires que le chèque contient déjà [8, 14, 1]. Néanmoins, le chèque peut être considéré comme **divisible** car, n'importe quel montant peut y être inscrit pour peu que les fonds nécessaires soient disponibles.

Il répond aussi aux exigences des institutions financières de par son exactitude lors des transactions et sa praticabilité lors des paiements de grosses sommes.

Cependant, le chèque est sujet à des **menaces** de nature **intentionnelle** et **active** qui sont principalement, la falsification (modification du montant d'un chèque par le porteur, émission du chèque par une autre personne que son tireur) et l'émission d'un chèque sans provision (le tireur remet au porteur un chèque dont il sait qu'il ne peut être tiré) [8, 27, 28].

[6] http://www.cba.ca/index.php

Somme toute, nous pouvons dire que sa simplicité d'utilisation, le fait qu'on puisse effectuer des paiements de montants élevés sans pour autant être encombré de nombreuses coupures, l'encaissement des paiements pouvant être différé ou encore le fait qu'un chèque perdu peut être annulé ou réémis en font un moyen de paiement avantageux [14, 1.12]. À contrario, au nombre de ses inconvénients on peut citer le fait qu'il ne protège pas l'anonymat ou qu'il ne soit accepté que par de rares commerçants. De plus, un tiers mal intentionné pourrait utiliser des chèques perdus ou volés pour effectuer des ordres de paiements, ce qui peut engendrer des pertes pour le commerçant en cas de contestation du véritable propriétaire [1.12, 14].

Un autre désavantage et non des moindres, est qu'il demeure tout de même onéreux pour les institutions financières qui doivent en assurer l'émission, la sécurisation et la conservation [18]. De ce fait, pour en amoindrir les coûts, elles les font payer aux utilisateurs.

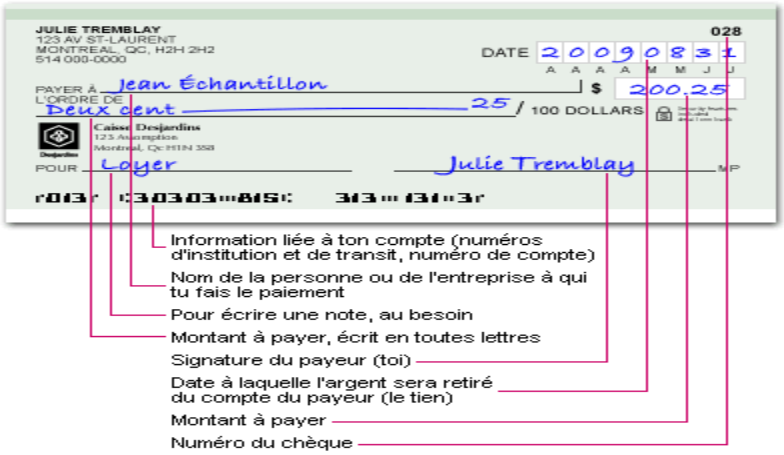

Figure 1.3. Caractéristiques d'un chèque [1.11]

Nous avons vu dans ce chapitre, tout d'abord les termes et les notions qui seront utilisés dans les chapitres suivants. Ensuite, le fonctionnement général des moyens de paiement ainsi que les propriétés qui serviront de base comparative pour l'analyse de ces derniers ont été explicités. Enfin, la caractérisation et l'analyse des deux moyens de paiement considérés comme traditionnels ont servi à conclure ce chapitre.

Ainsi, le prochain chapitre amorcera la partie technique de ce travail, en traitant des notions et techniques cryptographiques ayant permis l'avènement de nouveaux moyens de paiement.

Chapitre 2. Notions et techniques cryptographiques.

À la différence des moyens de paiement dits « traditionnels », il en existe d'autres qui sont eux, électroniques. Ces derniers utilisent des notions et techniques cryptographiques qui feront l'objet de ce chapitre. Ainsi, non seulement nous expliquerons certains protocoles mais également les différents types d'identification et d'attaques. Aussi, la confidentialité des réseaux, les fonctions de hachages cryptographiques et les codes d'authentification de messages seront décrits avant de conclure par l'authentification à l'aide de la signature numérique.

2.1. Protocoles.

Un protocole cryptographique est un mode de communication utilisant des algorithmes cryptographiques et impliquant au moins deux parties, une partie étant prise comme une personne ou un ordinateur [29, 30]. De plus, lorsque celle-ci reçoit ou manipule de l'information, elle est appelée « entité ».

Les protocoles d'identification, quant à eux, consistent en des échanges entre le client ou prouveur P et le serveur ou vérificateur V. P doit certifier son identité à V qui lui est en charge de l'approbation de cette dernière. Il revient donc au prouveur de s'authentifier auprès du vérificateur [31]. Ces protocoles sont mis en place pour parer les réseaux informatiques contre les éventuelles attaques auxquelles ils doivent faire face.

2.2. Attaques et protocoles d'identification.

2.2.1. Différents types d'attaques.

L'élaboration d'un système informatique sûr requiert l'identification des possibles attaques qu'il pourrait être amené à subir et les méthodes pour y remédier. En effet, cette analyse est indispensable pour entraver la vulnérabilité du système. De ce fait, on distingue différents types d'attaques, regroupés selon plusieurs standards. Le classement du standard X.800, présenté ici, les regroupe en deux grands ensembles, à savoir les attaques passives et actives [8].

D'une part, les **attaques passives** sur un système informatique sont celles où un tiers non-autorisé dénommé « adversaire » essaie d'obtenir une information confidentielle en écoutant passivement les communications [2.1]. Il n'existe que deux façons de les mener à bien : Soit en utilisant l'**attaque de l'homme du milieu** qui consiste pour l'adversaire à se positionner entre l'expéditeur et le destinataire d'un message afin de l'intercepter, ces derniers croyant communiquer l'un avec l'autre ne s'en aperçoivent pas [7 , 32]; Soit grâce à l'**attaque par analyse de fréquence** au cours de laquelle l'adversaire réussit à accéder à une information en décryptant les données interceptées à travers une analyse de la longueur des mots [2.2, 32]. Ce genre d'attaque est certes difficile à détecter car, ne laissant que très peu d'indices, mais elles peuvent être repoussées principalement par l'utilisation du chiffrement et d'autres techniques comme les mixnets et le routage en oignon (par exemple Tor). En outre, la sténographie peut également convenir [7] .

D'autre part, les **attaques actives** sont caractérisées par la participation de l'adversaire dans le déroulement normal des opérations [8]. Ce sont les plus courantes et celles qui causent le plus de dégâts, car elles impliquent la modification des données ou leur création. Les recommandations X.800 recensent deux moyens de les réaliser : Soit en utilisant les **attaques par redite** durant lesquelles l'adversaire répète seulement une partie ou un message entier intercepté pendant une communication, et ce avec pour objectif d'accéder à une information [32]; Ou alors les **attaques par modification des messages** qui consistent à altérer un message original ou à le réorganiser, sans que cela ne soit détecté, dans le but de produire un effet non-autorisé. De plus, il arrive parfois que le message soit différé [32]. Les attaques actives sont les plus difficiles à contrer. Toujours selon les recommandations X.800, des combinaisons de mots de passe et de chiffrement ou des moyens cryptographiques (codes d'authentification de messages, signatures numériques) peuvent assurer la protection nécessaire. Plus spécifiquement, pour les attaques par redite, les méthodes de marquages temporels[7] (timestamps) ou de défis imprévisibles et à usage unique sont utilisées [2.3].

[7] Les marqueurs temporels sont des données temporelles (date, heure) ajoutées aux messages dans des protocoles cryptographiques pour éviter qu'une entité ne réutilise un message précédemment utilisé.

2.2.2. Identification par mots de passe et par preuve de connaissance interactive à divulgation nulle.

Un **mot de passe** est une série de caractères transmis de façon chiffrée par P à V. Il permet à ce dernier d'identifier P de façon sécuritaire ou d'assurer la confidentialité des communications entre les deux entités [31]. Le Numéro d'Identification Personnel (NIP) qui est un type de mot de passe et la signature du reçu d'un achat par carte de crédit sont deux moyens prisés des institutions financières pour authentifier leurs utilisateurs [31, 2.4]. Cependant, il n'en demeure pas moins qu'il existe d'autres modes d'authentification. Par exemple, si au terme de l'exécution de l'identification, le vérificateur peut établir que le prouveur dispose de l'information privée *sp* sans que celle-ci lui ait été dévoilée, alors il s'agit d'une identification **par preuve de connaissance à divulgation nulle** [30].

2.3. Confidentialité des données d'un réseau.

La confidentialité des données qui transitent sur un réseau est principalement garantie par deux formes de chiffrements. Il s'agit du chiffrement asymétrique ou à clé publique et du chiffrement symétrique ou à clé privée; Ceux-ci aident à protéger les données dudit réseau de certaines attaques.

2.3.1. Chiffrement symétrique.

Pour parler de chiffrement symétrique, il faudrait tout d'abord en définir les composantes. C'est alors que le chiffre à utiliser $\Pi\ (E, D, G)$ doit être un triplet d'algorithme où, G sera un générateur de clé tel que : $k \leftarrow G\ (1^n)$. Ainsi, nous proposerons les éléments suivants : E l'algorithme de chiffrement, D l'algorithme de déchiffrement, M l'espace de message, m un élément de M, C l'espace de chiffrement et c un élément de C et $G\ (1^n)$ l'ensemble des clés .

Partant de ces faits, un chiffre $\Pi(\ G, E, D)$ est dit symétrique ou à clé privée, si la clé k associée respectivement aux fonctions de chiffrement $E_k(m)$ et de déchiffrement $D_k(c)$ est la même, de telle sorte que le chiffre c du message m est [26, 33] :

$$c = E_k(m);$$

Et inversement : $m = D_k(E_k(m))$ [2.5, 2.6, 33].

2.3.2. Chiffrement asymétrique.

Un chiffre $\Pi(G, E, D)$ est dit asymétrique ou à clé publique si et seulement si, à chaque clé publique de chiffrement *pk* correspond une clé secrète *sk* de déchiffrement du message *m*. Cette opération aboutit à la constitution d'une paire de clés *(pk, sk)*. Le principe de ce système réside dans la difficulté à déterminer *sk* à partir de la seule clé *pk,* puisqu'elle est publique. On obtient ainsi les algorithmes de chiffrement et de déchiffrement suivants [29, 33, 32] :

Chiffrement : $E_{pk}(m) = c$,

Déchiffrement : $D_{sk}(c) = D_{sk}(E_{pk}(m)) = m$.

2.3.3. Exemple de chiffrement asymétrique : le chiffrement RSA.

Sorti des laboratoires du Massachusetts Institute of Technology (MIT), en 1977, le chiffrement RSA est le plus utilisé de nos jours. C'est l'acronyme des noms de ses inventeurs Rivets, Shamir et Adleman [7] . Basé sur deux clés, une publique et une autre privée, le chiffrement RSA se présente selon la suite d'équations suivante [30, 33, 34, 35]. Soit alors une clé publique *pk* ayant deux nombres *(N, e)* avec :

$$N = pq$$

Où *p* et *q* sont deux nombres premiers de taille similaire;

Et $e > 1$ et le PGCD $(\varphi(N), e) = 1$ (avec e $\epsilon\ \mathbb{Z}*_{\varphi(N)}$).

avec $\mathbb{Z}^*$ l'ensemble des entiers relatifs non nul et φ^N la valeur de l'indicatrice de Euler en N.

Soit aussi une clé privée *sk = d*, associée à la clé publique (N, e) telle que:

$$d \epsilon\ \mathbb{Z}*_{\boldsymbol{\varphi(N)}} \text{ et } ed = 1 \bmod \varphi(N).$$

Dès lors, le chiffrement du message $m \in \mathbb{Z}*_N$ avec le système RSA sera:

$$c = m^e \bmod N$$

Inversement, le déchiffrement à partir de la clé privée *d*(c $\in \mathbb{Z}*_N$) obtenu en utilisant la fonction d'Euler [8] [32, 34, 37, 2.7, 2.8] se déroulera de la façon suivante :

$$c^d \bmod N = (m^e \bmod N)^d \bmod N$$
$$= m^{ed} \bmod N = m^{k\varphi(N)+1} \bmod N$$

[8] http://math-it.org/Mathematik/Zahlentheorie/Euler.html.

$= (m^{\varphi(N)}) \; mod \; N \; \times \; m \; mod \; N$

$= 1^k \times m \; mod \; N = m.$

2.4. Fonction de hachage et Code d'authentification des Messages.

Une **fonction de hachage** cryptographique est facile à calculer mais difficilement inversable, ce qui en fait une fonction à sens unique telle que :

$$h: \{0,1\}^* \rightarrow \{0,1\}^n$$

Cette fonction transforme un message *m* de taille quelconque en un message *h*, $\in \{0,1\}^n$de taille fixe inférieure au *m* original appelé « empreinte de sortie » ou condensat [36, 29, 37]. Elle s'exprime comme suit :

$$h(m) \; = \; h.$$

Considérant que $m \in \{0,1\}^*$, il doit aussi être impraticable de trouver un message *m*' différent de *m* tel que :

$$h(m) \; = h(m').$$

Et

$$h = h(m).$$

De fait, une fonction de hachage satisfaisant $h = h(m)$ est dite résistante aux collisions [37, 35, 2.7].

En outre, les fonctions de hachage produisent des messages d'authentification pouvant être menacés. Par exemple, un individu malveillant peut à la fois modifier les données originales et le condensat, le **Code d'Authentification de Messages** (CAM), en en précisant la source, permet de contrecarrer ces risques [36].

En effet, plus connu sous son acronyme anglais MAC, le code d'authentification des messages est un système associant une fonction de hachage *h(m)* et une clé secrète *sk* dans lequel, l'expéditeur et le destinataire possèdent la même clé secrète [36]. C'est ainsi que le premier envoie le message *m* suivi de l'appendice *a = h (m, sk)* au second, qui doit le vérifier par le calcul de *h (m, sk)*; le résultat de cette opération conduire à l'appendice *a* reçu [36, 2.8, 2.9].

Mis à part les CAM, d'autres méthodes permettent de certifier la provenance des messages comme les signatures numériques que nous verrons au point suivant.

2.5. Signature numérique.

Tel que mentionné plus haut, l'authentification des données est également rendue possible par l'utilisation de la signature numérique. Outre ce fait, elle en assure aussi l'identification, la non répudiation et la non réutilisabilité [37]. Axée sur la cryptographie asymétrique, la signature numérique est une fonction résistante aux collisions, généralement utilisée en hache-et-signe pour des messages de longueurs arbitraires [38].
Elle est définie par le processus ci-après :
Soient *m* un message, *K* un ensemble de paires de clés (*pk, sk*) où *pk* est publique et *sk* privée. *S* est un algorithme qui génère une signature pour un *m* à partir de *sk,* définie par $S_{sk}(m)$. *V* en est un autre qui, lui, vérifie une signature *s* pour *m* à partir de la clé publique *pk* de l'expéditeur du message. Le protocole est alors traduit comme suit :

$$V_{PK}(m, S_{sk}(m)) = 1,$$

$$V_{pk}(m, s) = 0 \; si \; s \neq S_{sk}(m)$$ [33, 35, 38, 39].

Ainsi, de façon pratique, pour signer un message de longueur quelconque, le système commence d'abord par calculer l'empreinte h de m à travers une fonction de hachage cryptographique H tel que: $h = H(m),$ puis signe m comme suit:

$$S_{sk}(m) = S_{sk}(h)$$

Partant de cela, sa fonction de vérification est :

$$V_{pk}(m, S_{sk}(m)) = vrai \iff S_{sk}(h) = S_{sk}(H(m)).$$

Il est à noter qu'il existe plusieurs procédés de signature numérique. C'est dans ce sens que nous présenterons dans les sous-sections ultérieures les procédés de signature RSA et numérique à l'aveugle.

2.5.1. Procédé de signature RSA.

De ce qui précède, il est évident que le chiffrement RSA s'effectuera à l'aide des clés publique et privée *(pk, sk)* tel que: *(pk, sk) = ((N, e), d)*. Partant de cela, le signataire connait *sk,* tandis que les vérificateurs, eux, ont connaissance de *pk*. La signature du message *m* est alors [29, 2.2, 33, 39]:

$$S_d(m) = m^d mod\ N = s.$$

(m, s) étant un message avec signature.

Tandis que la vérification du message (M, s) est:

$$V_{pk}(m,s) = \begin{cases} Vrai\ si\ s^s mod\ N = m \\ Faux,\ sinon. \end{cases}$$

2.5.2. Signature numérique à l'aveugle.

Inventé par le cryptographe David Chaum[9], le protocole numérique de signature à l'aveugle dérive du RSA. Au cours de celui-ci, le signataire utilise un algorithme de chiffrement à clé publique pour signer un message dont il ignore le contenu. De ce fait, considérant un client *U,* qui veut faire signer sa pièce *m* de façon aveugle par une banque *B,* ayant en sa possession un module public *n* et deux clés, une publique *e* et une privée *d*, de telle sorte que *(pk, sk) = ((n, e), d)* et *d = * d^{-1}*. Ce protocole se déroulera alors de la manière suivante [37, 40, 2.10] :

1. *U* choisit au hasard un facteur de camouflage *r* compris entre 1 et *n* pour que *m* soit ensuite masqué selon la formule ci-après :

$$P = m*r^e \ (mod\ n);$$

2. *U* envoie par la suite le message masqué *P* à *B* qui le signe avec sa clé privée comme suit:

$$P^d = (mr^e)^d\ mod\ n = m^d r\ mod\ n;$$

3. Après cette étape, *B* retourne *P* à *U* qui se chargera d'extraire le message de paiement signé, en utilisant la fonction de démasquage *C*. Cette opération consiste à diviser *m* par *r* avant de s'assurer que le message envoyé à *U* est identique à celui reçu selon la fonction ci-dessous :

$$C = P^d / r\ (mod\ n) = m^d\ (mod\ n)$$

4. *U* aura alors comme résultat final de la signature:

$$C = m^d\ mod\ n$$

[9] Cryptographe, Fondateur et membre du conseil d'administration de Digicash Inc. http://www.chaum.com/welcome.html

Étant le point de départ de tous les principes de base ayant trait à la conception d'une monnaie électronique anonyme, le déroulement d'un protocole de signature à l'aveugle est donné en exemple par la figure 2.1.

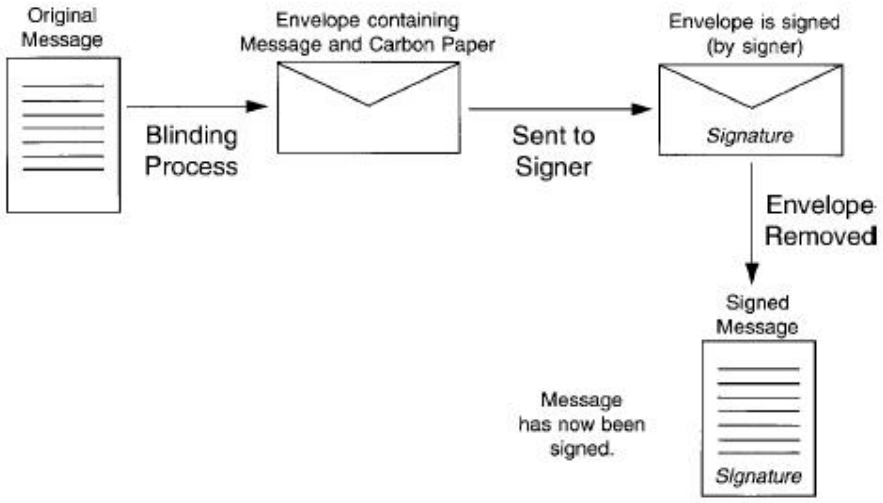

Figure 2.1. Exemple de protocole de signature à l'aveugle [40].

Ayant présenté les notions et les techniques cryptographiques permettant la création de nouveaux moyens de paiement, nous verrons au cours des prochains chapitres comment ces techniques seront appliquées aux moyens de paiement dits « électroniques ».

Chapitre 3. DigiCash et Bitcoin.

Comme nous l'avons précédemment évoqué, outre les moyens de paiement dits « traditionnels», il en existe d'autres qualifiés, eux, d'«électroniques». Citons en exemple la monnaie électronique, issue des travaux des pionniers dans le domaine de la cryptographie, dont David Chaum, fondateur de DigiCash [3.1, 9]. Leur but était de produire un substitut à la monnaie fiduciaire, en en conservant les mêmes avantages, dont principalement l'anonymat et l'offline [41, 3.2]. En plus de DigiCash, les années 2009 et 2010 ont vu l'apparition d'un autre modèle de monnaie électronique, lui décentralisé et online, portant le nom de bitcoin, ayant pour principal objectif, une totale indépendance vis-à-vis des banques et des gouvernements [3.3]; si bien qu'il est primordial de nous attarder sur ces deux différents moyens de paiement au cours de ce chapitre.

3.1. DigiCash.

Basé sur le chiffrement RSA et le calcul des primitives cryptographiques, DigiCash a pour but d'offrir les mêmes avantages que la monnaie fiduciaire en matière d'anonymat et de non-traçabilité. Ces commodités sont acquises par l'entremise de sa monnaie électronique qu'est le e-cash [9, 42, 43]. Par conséquent, une analyse plus profonde s'impose mais, il convient avant tout de décrire le fonctionnement de ce système de paiement.

3.1.1. Fonctionnement.

De prime abord, il faudrait signaler que l'ouverture d'un compte bancaire dans une institution proposant DigiCash est une condition sine qua non à l'utilisation de ce système [44]. Le futur utilisateur pourra ensuite acheter des e-cash grâce au logiciel DigiCash gratuitement téléchargeable sur le site web de la société [5] . Ledit achat se fera via un transfert de son compte bancaire à un compte particulier de la banque DigiCash appelée « cyber-banque » (1). La monnaie électronique ainsi acquise peut, soit être stockée sur un disque dur, soit être laissée dans un compte spécial de la cyber-banque (2). Les paiements et autres achats peuvent dès lors être possible avec les e-cash (3).

C'est ainsi que le vendeur ou l'utilisateur de ces paiements peuvent, s'ils le désirent, transformer ces e-cash en devise courante auprès de la « cyber-banque » qui s'en chargera après effectuation de leur vérification (4) [40, 42, 45]. La figure 3.1., ci-après résume bien nos propos.

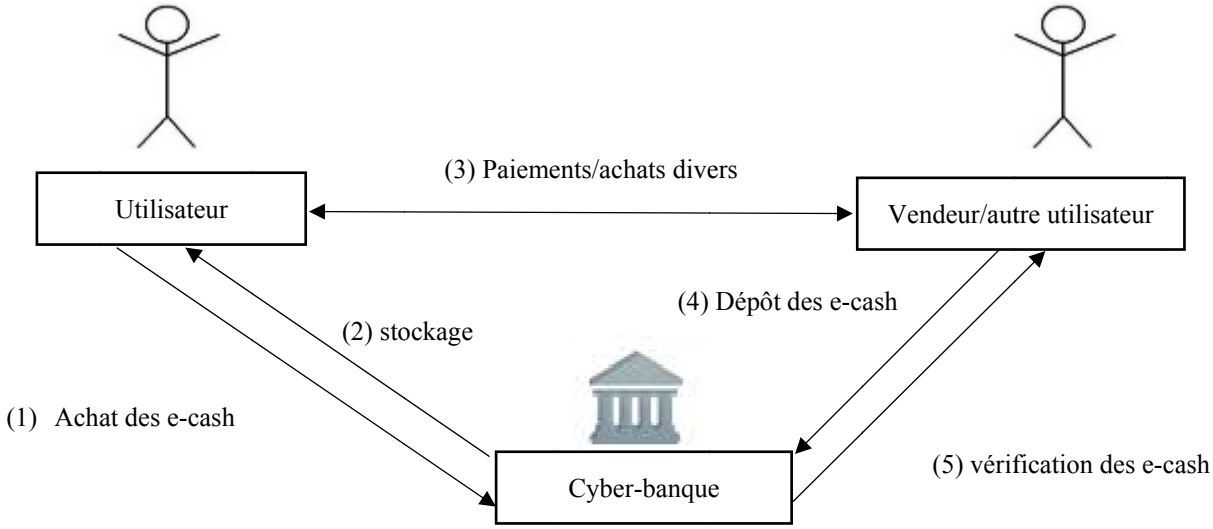

Figure 3.1. Fonctionnement de DigiCash [45]

Outre son fonctionnement global, DigiCash est axé autour de différents protocoles présentés au point 3.1.2.

3.1.2. Protocoles de retrait, d'achat et de détection de la double- dépense.

Les protocoles de retrait, d'achat et de détection de la double-dépense, proposés par Chaum, Fiat et Naor [43], seront développés ci-dessous. Soulignons que les deux premiers cités assurent l'anonymat et la non-traçabilité et sont issus du procédé de signature numérique à l'aveugle qui, pour rappel est lui-même dérivé de la signature RSA.

Tout d'abord, posons les éléments dont nous aurons besoin pour expliciter ces protocoles.

Soient alors :$(pk, sk) = ((N,e),d)$;

e, la clé publique de la banque ;

d, la clé privée de la banque ;

N, le module RSA avec $N=pq$ (p et q étant des nombres premiers impairs) et de taille suffisante ;

k, le paramètre de sécurité ;

f et g, *deux* fonctions à sens unique sans collision possédant chacune deux arguments; u, le numéro de compte du client U et v le compteur associé au numéro de compte d'U

$\oplus$: Opérateur xor, || : concaténation.

3.1.2.1. Protocole de retrait anonyme.

Le protocole de retrait anonyme se déroule en six étapes, à savoir:

1. U choisit de façon aléatoire a_i, c_i, d_i et r_i *(mod N)* avec $(1 \leq i \leq k)$;

2. Ensuite, U forme et envoie à la banque un nombre k de possibles messages de paiement masqués candidats, de sorte que:

$$P_i = r_i^e * f(x_i, yi)\ (mod\ N)\ (1 \leq i \leq k),$$

Où:

$$x_i = g(a_i, c_i) \text{ et } y_i = g(a_i \oplus (u \,||\, (v+i)), d_i)\ ;$$

3. Suite à cela, B choisit aléatoirement un sous-ensemble $k/2$ des k messages dans l'ensemble $R = \{i\}_j$, $\{i_1, i_2, \ldots, i_{k/2}\}$, avec :

$$R = \{k/2+1, \ldots, k\};$$

4. U doit à ce stade révéler a_i, c_i, di *et* r_i pour tout $i \in R$ afin que, B vérifie si cela peut former P_i ;

5. D'où, B donne à U selon l'équation :

$$\prod_{i \notin R} P_i^d \ mod\ N = \prod_{1 \leq i \leq k/2} P_i^d \ mod\ n$$

Avant de charger le compte de U du montant correspondant tout en incrémentant le compteur v du compte u de U par k ;

6. Finalement, U peut alors incrémenter sa copie de v par k après avoir extrait le billet électronique en utilisant la fonction de démasquage C, tel que:

$$C = \prod f(x_i, y_i)^d mod n,\ 1 \leq i \leq k/2;$$

3.1.2.2. Protocole d'achat.

Le protocole d'achat se produit d'après les cinq étapes ci-après :

1- Tout d'abord, *U* envoie *C* à *S*;

2- Ensuite, *S* choisit une chaine de bits aléatoires $z_1, z_2, ..., z_{k/2}$ avant de les envoyer à *U*;

3- D'où, *U* répond, pour tout $i \leq i \leq k/2$, selon les deux alternatives suivantes :

- si $z_i = 1$, alors *U* envoie à *S* a_i, c_i et y_i ;
- si $z_i = 0$, *U* envoie donc à *S* x_i, $a_i \oplus (u||(v+i))$ et d_i ;

4- Suite à cela, *S* vérifie que *C* est correct et correspond bien à celle reçue de *U* en calculant $f(x_i, y_i)$ et en vérifiant la signature de la banque;

5- *S* envoie enfin *C* et la réponse de *U* à la banque, qui vérifie sa véracité et crédite son compte ;

C'est ainsi que *B* doit conserver *C*, $z_1, ..., z_k$ et a_i (pour $z_i = 1$) et $a_i \oplus (u||(v+i)$ (pour $z_i = 0$).

3.1.2.3. Détection de la double-dépense.

L'anonymat des transactions dans le système DigiCash a créé le problème de la double-dépense, en ce sens qu'il est facile de contrefaire la monnaie électronique. Pour cela, il suffit de copier le fichier la contenant [44]. Stefan Brand's est celui qui a découvert cette faille de sécurité et il en proposa des solutions. Cependant, et ce dans une optique de continuité, la solution présentée ici sera celle de Chaum, Fiat et Naor.

Pour ce faire, en se basant sur les deux protocoles précédents, ces derniers facilitent la détection de la double-dépense. En effet, si *U* utilise le même billet électronique deux fois, il existe une très grande probabilité que deux *S* distincts envoient des valeurs différentes pour un même z_i;

Après comparaison, la banque peut trouver le compte *u* correspondant, sachant qu'elle connaît à la fois a_i et $a_i \oplus (u||(v+i))$.

3.1.3. Analyse de DigiCash.

Analyser DigiCash reviendrait à se servir de certains des critères utilisés relativement aux analyses des monnaies traditionnelles, afin d'en mettre en évidence les avantages et les inconvénients.

Ainsi, les concepteurs de DigiCash ont très vite compris qu'il fallait prévenir la double-dépense pour acquérir la **confiance des utilisateurs**. Plusieurs méthodes de détection furent éditées dont celle de Chaum, Fiat et Naor présentée précédemment. En plus de celles-ci, il a été recommandé aux vendeurs de procéder au dépôt immédiat de la monnaie numérique perçue à la cyber-banque [44, 41]. En outre, mentionnons que la cryptographie asymétrique, sur laquelle repose ce système, en intensifie la sécurité.

Aussi, notons qu'en dehors du fait qu'au Canada en général, les banques soient soumises aux lois canadiennes sur la protection des renseignements personnels, [1.13] les banques québécoises sont de surcroît enclines à respecter les lois québécoises sur la protection des renseignements personnels dans le secteur privé [26]. Toutes les informations personnelles collectées ne peuvent être utilisées sans le consentement du titulaire du compte. Hormis cette position juridique, la **protection de la vie privée** est renforcée par l'utilisation de la signature à l'aveugle sur le e-cash, évitant ainsi tout lien direct avec le compte utilisateur [46]. De plus, la **non-traçabilité** que procurent les divers protocoles de DigiCash autorise la dissociation d'un e-cash de l'identité de son utilisateur, garantissant ainsi l'**anonymat**.

Toutefois, les transactions sur DigiCash ne respectent aucune des propriétés **ACID** définies au chapitre 1. Tout d'abord, elles ne sont pas atomiques car, en cas d'interruption du système, le statut d'une transaction n'est connu d'aucune des parties prenantes; Ceci étant dû au fait qu'elles ne sont pas nécessairement informées de l'état du paiement [45]. Cette situation compromet les propriétés de cohérence et d'isolation. En effet, le marchand et le client pouvant clamer, pour l'un que la transaction n'a jamais pris place et pour l'autre, qu'elle a bel et bien été complétée. Par ailleurs, ces transactions ne sont pas durables, en ce sens qu'une fois qu'un e-cash a été déposé à la banque, il est retiré de la circulation sans être conservé dans un historique [45, 44]. Le e-cash peut cependant être considéré divisible, puisque le client conçoit et génère la monnaie électronique dont il a besoin en équivalence d'une unité de monnaie nationale. Ainsi, ce dernier pourra produire des e-cash de différentes valeurs selon ses besoins [47, 43].

Suite à cette analyse, nous sommes arrivés à la conclusion que le système DigiCash avait ses avantages. Assurément, il semblait être l'alternative parfaite à la monnaie fiduciaire.

L’anonymat de ses transactions, la sécurité et le respect de la vie privée qu’il offrait en faisait un moyen de paiement bénéfique pour ses utilisateurs [9, 47]. Cependant, malgré les aspects positifs énumérés, DigiCash n'a pas réussi à s'imposer. En effet, des inconvénients ont subsisté.

Le fait que l’effectuation des opérations requiert des protagonistes qu’ils soient clients de la même banque et la non-traçabilité de ses transactions qui rendait impossible toute contestation, ont contribué à passer sous silence DigiCash [44].

Outre cela, cet insuccès est aussi en grande partie imputable au fait qu'il était en avance sur son temps. Une adaptation des systèmes bancaires était donc requise alors qu’elle était jugée non nécessaire par les banques [3.4]. L’incompréhension causée par la complexité du système et la lourdeur des calculs lors des transactions ont participé au flop commercial de DigiCash [48]. Aussi, le quasi-manque d’intérêt du public était supporté par le fait que le e-cash n’était accepté que dans très peu d’institutions.

3.2. Bitcoin.

Le bitcoin est la première monnaie numérique non-émise par un gouvernement ou tout autre genre d’organisme public ou privé. Mis en place par un développeur connu sous le pseudonyme de Satoshi Nakamoto et publié en Octobre 2008, il ne sera effectif qu’à partir de janvier 2009 [49, 3.5, 3.6, 3.7]. Vu son envergure et de son audace, le bitcoin se doit d’être analysé, mais avant il faut en décrire le fonctionnement et les divers constituants.

3.2.1. Fonctionnement.

Le bitcoin fonctionne sur un réseau pair à pair dans lequel il partage un grand journal comptable dénommé « chaine de blocs » qui contient tous les échanges effectifs [3.8]. Ceci permet de vérifier la validité de toute transaction avant de l’entériner.

Pour utiliser bitcoin, il faut en télécharger le logiciel sur un support électronique (ordinateur, téléphone intelligent …) qui génèrera la première adresse bitcoin et permettra d’en créer de nouvelles. Ces adresses authentifieront les transactions, chaque bitcoin correspondant à une signature numérique de l’adresse émettrice [50].

De plus, les utilisateurs peuvent gagner des bitcoins, en mettant au service du réseau, la puissance de calcul de leur machine. Ce procédé s'appelle le « minage » [3.8].

3.2.2. Chaine de blocs.

En conservant chronologiquement toutes les transactions validées sur le réseau après des calculs complexes appelés « preuve de travail », la chaine de blocs résout le problème de la double-dépense [50, 51].

En effet, chaque bloc contient le hach du précédent, donnant la possibilité aux utilisateurs de vérifier que les nouvelles transactions n'utilisent pas de bitcoins contrefaits en les comparants à ceux contenus dans la chaine de blocs [3.9]. La figure 3.2. en donne un exemple représentatif.

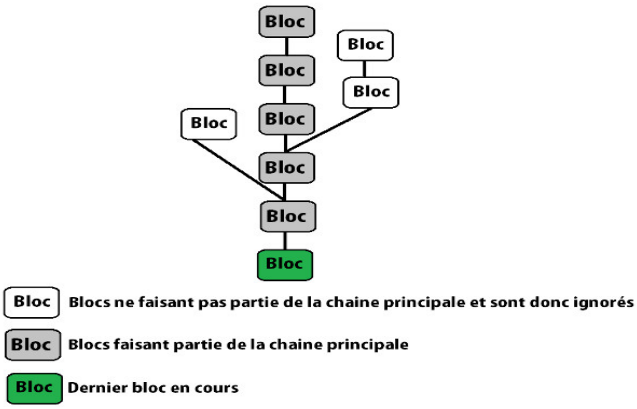

Figure 3.2. Chaine de blocs bitcoin [3.10]

3.2.3. Transactions bitcoin.

Un bitcoin est représenté comme une chaine de signatures. Ainsi, pour effectuer une transaction, l'expéditeur signe non seulement l'empreinte de la précédente, mais aussi la clé publique du destinataire qu'il rajoute à la fin du bitcoin [3.6]. Ceci permet au destinataire de vérifier l'authenticité du bitcoin et sa provenance avant de le valider [3.9, 3.11]. La figure 3.3. ci-dessous résume ce protocole.

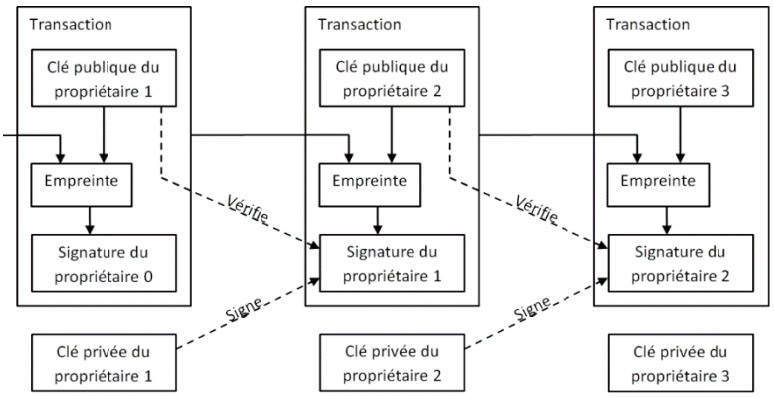

Figure 3.3. Fonctionnement d'une transaction bitcoin [3.12].

3.2.4. Validation des transactions bitcoin : Minage.

Pour être validée, une transaction doit être vérifiée puis admise dans un bloc. Cette opération appelée « minage » s'effectue à travers des preuves de travail consistant, par exemple, à déterminer une valeur x débutant par un certain nombre de bits à 0 en utilisant SHA 256 [3.6, 52, 3.13]. Cette procédure rend le calcul extrêmement difficile en fonction du nombre de bits à 0 demandés, mais peut être validée en effectuant un unique calcul d'empreintes. La preuve de travail rend l'altération ou la duplication d'un bloc irréaliste, en ce sens que cela demanderait du temps et une puissance de calcul énormes. De plus, les blocs sont aussi renouvelés toutes les dix minutes, pour assurer la neutralité du réseau, évitant ainsi qu'une machine n'en ait le contrôle [3.3]. La figure 3.4. ci-après montre une preuve de travail.

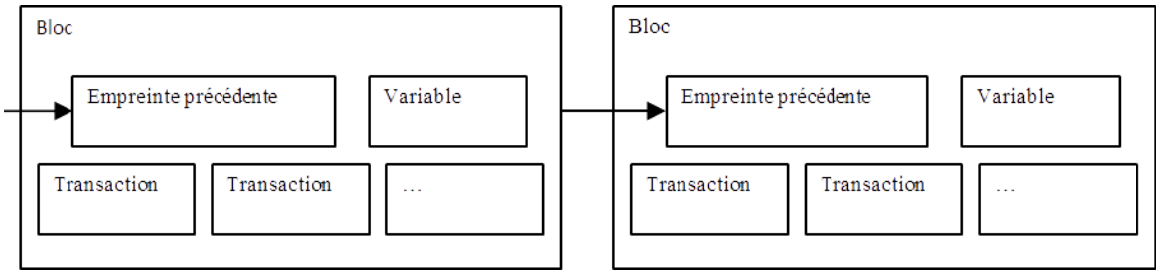

Figure 3.4. Preuve de travail [3.12].

3.2.5. Analyse de bitcoin.

Cette observation sera basée sur les mêmes aspects que précédemment à savoir que, pour acquérir la **confiance des utilisateurs**, le concepteur de bitcoin s'est arrangé à avoir un risque de fraude minime. Pour cela, il a axé son système sur le minage, la preuve de travail et les chaines de blocs [3.6]. Ces mécanismes de sécurité engendrent la confiance des utilisateurs vis-à-vis du système.

Malheureusement, bitcoin est basé sur la publication de toutes ses transactions, ce qui en fait un système ouvert et donc insoumis aux lois sur la **protection sur la vie privée.** De ce fait, il ne la garantit nullement [3.14]. Tous les utilisateurs d'un réseau pourraient connaitre le solde d'un compte et la nature de transactions ne les concernant pas [51]. En dépit de cela, il peut être considéré comme un système partiellement **anonyme**.

En effet, chaque transaction contient la date, l'adresse bitcoin et la somme versée. Il est alors possible, en retraçant toutes les adresses bitcoins d'un utilisateur et en effectuant une analyse minutieuse des données de ses différentes transactions, d'avoir accès à son identité réelle [53] ; D'où l'importance d'utiliser un porte-monnaie bitcoin en ligne qui brouille de façon automatique les soldes en croisant les transactions entre ses utilisateurs.

En outre, se basant sur la définition des propriétés **ACID** et de ce qui précède, il est aisé de conclure que les transactions bitcoin sont atomiques. En effet, elles sont complétées entièrement ou pas du tout. Elles sont de plus cohérentes, en ce sens que, la dépense d'un bitcoin entraine son transfert du compte de l'acheteur vers celui du vendeur. Ainsi, le système passe d'un état A à un état B, tous deux valides. Ces transactions sont également isolées car, pour deux transactions réalisées au même instant, il n'y a pas de conflit. Enfin elles sont durables, parce qu'inscrites de façon définitive dans le journal des transactions. De surcroît, bitcoin est **divisible** et ce jusqu'à huit chiffres après la virgule. Ainsi, la plus petite unité de bitcoin est 0. 0000 0001 [54].

Hormis tout cela, le bitcoin ne cherche pas à 'plaire' aux institutions financières, il se veut un moyen de paiement indépendant et décentralisé. Cet état de fait lui permet de n'être soumis à aucune régulation institutionnelle, ce qui a pour effet d'engendrer une certaine inquiétude. Pour exemple, la banque de France le qualifie de monnaie « hautement spéculative » avec un « risque financier certain » [55].

En conclusion, les **institutions financières** n'ont aucune **attente** envers bitcoin, elles le craignent plutôt, entrainant ainsi de fortes pressions de la part des gouvernements. En effet, certains pays comme la France essaient de le réguler [3.16]; Tandis que la Russie demeure dubitative quant à sa suspension, et que l'Inde et la Chine l'ont tout simplement banni [3.17]. Ceci a des répercussions considérables sur le cours du bitcoin. Excepté ces écueils institutionnels, les principales **menaces** pesant sur bitcoin sont le piratage et le vol. Pour exemple, plus de cinq cent millions de dollars américains en bitcoin (500 000 000 $) ont été dérobés à la bourse de bitcoin, MtGox. Une autre bourse, bitfloor, a subi une attaque ayant occasionné le vol de deux cent cinquante mille dollars américains (250 000 $) [3.15].

Malgré cela, nous pouvons dire que bitcoin regorge de nombreux avantages comme le fait que son utilisation ne demande aucun frais de transferts; Ceux-ci se faisant de façon rapide et sans délai. Aussi, il permet le stockage et le transfert de fonds sans l'intervention d'un tiers; les transactions sont, de ce fait, confidentielles et soumises au contrôle total des utilisateurs [54]. Citons aussi l'irréversibilité des transactions, qui présente peu de risques pour le vendeur et encore moins pour l'utilisateur, car elles ne contiennent aucune information sensible ou personnelle [54].

Cependant, il a aussi de nombreux inconvénients. En effet, il est à noter que l'utilisation de bitcoin requiert une certaine compréhension technique du système. Rajouté à cela, le nombre de commerces le proposant demeure très limité [54]. L'irréversibilité des transactions, tantôt présentée comme un bénéfice, associée à l'anonymat s'avère problématique pour les utilisateurs. Par exemple, un achat réglé et non-reçu ne peut faire l'objet d'une contestation.

Dans ce chapitre, nous avons présenté deux moyens de paiement électroniques assez singuliers dans leur fonctionnement que sont le système Digicash et bitcoin. Le chapitre suivant, nous permettra d'aborder un tout autre moyen de paiement électronique qu'est le paiement par carte.

Chapitre 4. Cartes de paiement à puce.

C'est en 1968, que deux ingénieurs allemands, Jurgen Dethoff et Helmut Grotrupp introduisent l'idée d'incorporer une puce à l'intérieur d'une carte en polychlorure de vinyle (pvc) [56]. Dès 1969, ils en déposent un brevet. En 1970, le natif du Japon, Kunitaka Arimura de l'Institut Arimura Technology, dépose lui-aussi dans son pays un brevet relatif à la carte à puce [57]. Par la suite, aux USA, l'année 1970 voit par Paul Castrucci de IBM, le dépôt d'un autre brevet concernant la carte à puce, intitulé « Information Card ».

Toutefois, les réelles avancées du domaine sont dues aux 47 brevets déposés, dans 11 pays différents entre 1974 et 1979, par le français Roland Moreno. Ces derniers mentionnent également les diverses applications possibles de la carte à puce [58]. En 1979, le groupe Bull commercialisait la première carte à puce; Celle-ci disposait d'une unité centrale et d'une mémoire programmable.

En 1983, cependant, les cartes de France Télécom, seulement dotées de simples mémoires, constituent la première véritable application du dispositif [58].

De nos jours, les cartes à puce sont utilisées dans de nombreux domaines tels que les télécommunications, les systèmes bancaires, les services de santé et les transports [59].

Néanmoins, dans ce chapitre, nous n'aborderons que le domaine financier en analysant les deux principaux moyens de paiement que sont les cartes de débit et de crédit afin d'en mettre les avantages et les inconvénients en lumière. Pour cela, les standards et les différentes formes de cartes à puce, ainsi que leurs caractéristiques et leurs sécurisations en général seront présentés. Les normes Eurocard Mastercard Visas (EMV) [Annexe C] renforçant la sécurité des cartes de paiement, seront également expliquées.

4.1. Standard des cartes à puce.

L'uniformité des cartes à puce est régie par des lois. En effet, les normes ISO/IEC/7816 définissent, entre autres, les caractéristiques physiques, l'emplacement des contacts, les fonctions et les emplacements des micromodules, mais également le niveau électrique, les ports d'entrées et de sorties ou encore l'application de l'information cryptographique. [60].

Ceci permet une utilisation à grande échelle de la carte à puce. Le tableau 4.1. donne un aperçu de ces normes.

Tableau 4.1. Liste des principales normes relatives aux cartes s'appliquant en totalité ou en partie aux cartes à puce [60]**.**

Normes ISO	Titre officiel	Traduction en français
ISO 7810	Identification Cards - Physical Characteristics	Cartes d'identification – Caractéristiques physiques
ISO 7811-1	Identification Cards – Recording Technique Embossing	Cartes d'identification – Techniques d'embossage
ISO 7811-2	Identifications Cards – Recording Technique Magnetic Stripe	Cartes d'identification – Techniques d'enregistrement magnétique
ISO 7811-3	Identification Cards – Recording Technique Location of Embossed Characters on ID 1 Cards	Cartes d'identification – Emplacement des caractères embossés sur les cartes de type ID 1
ISO 7811-4	Identification Cards – Recording Technique Location of Read-Only Magnetic Tracks – Tracks 1 and 2	Cartes d'identification – Position des pistes magnétiques à lecture seule – Pistes 1 et 2
ISO 7811-5	Identification Cards – Recording Technique Location of Read-Xrite Magnetic Tracks – Tracks 3	Cartes d'identification – Position des pistes magnétiques à lecture/écriture - piste 3
ISO 7812-1	Identification Cards – Identification of Issuers part 1: Numbering System	Cartes identification – Identification de l'émetteur, partie 1 : système de numérotation
ISO 7813	Identifications Cards – Financial Transaction Cards	Cartes d'identifications – Cartes pour transactions financières

Normes ISO	Titre officiel	Traduction en français
ISO 7186-1	Identification Cards – Integrated Circuit Cards with Contacts – Physical Characteristics	Cartes d'identification – Cartes à circuits intégrés avec contacts – Caractéristiques physiques
ISO 7186-2	Identification Cards – Integrated Circuits Cards with Contacts – Dimension and Location of the Contacts	Cartes d'identification – Cartes à circuits intégrés avec contacts – Dimension et position des contacts
ISO 7186-3	Identification Cards – Integrated Circuits Card with Contacts – Electronic Signal and Transmission Protocols	Cartes d'identification - Cartes à circuits intégrés avec contacts – Signaux électroniques et protocoles de transmission
ISO 7186-3 Amendement 1	Protocol type T =1, Asynchrones Half Duplex Block Transmission Protocol	Protocole T= 1, protocoles asynchrone semi-duplex à transmission par blocs.
ISO 7186-3 Amendement 2	Revision of Protocol Type Selection	Révision du mode de sélection de protocole
ISO 7816-4	Identification Cards - Integrated Circuits Cards with Contacts - Interindustry Commands for Interchange	Cartes d'identification – Cartes à circuits intégrés avec contacts - Commandes inter- industries
ISO 7816-5	Identification Cards - Integrated Circuits Cards with Contacts- Number System and Registration Procedure for Application Identifier	Cartes d'identification – Cartes à circuits intégrées avec contacts – Système de numérisation et procédure d'enregistrement pour l'identification des applications
ISO 1177	Information Processing – Character Structure for Start/Stop and Synchronous Character Oriented Transmission	Traitement de l'information - Structure des caractères pour les échanges synchrones orientés caractères

À ces normes, s'ajoutent les spécifications EMV qui, régissent les protocoles de communications, les instructions transmises ainsi que les données dans les cadres bancaire et financier [61] comme nous le verrons un peu plus tard.

4.2. Types de cartes à puce.

Il existe principalement trois types de cartes à puce, les cartes à mémoire, les cartes à microprocesseur et les cartes sans contact qui seront chacune présentées ci-dessous accompagnées d'un exemple du domaine de leur utilisation.

En premier lieu, intéressons-nous aux **cartes à mémoire** qui peuvent être subdivisées en deux sous-catégories [58]. La première étant celle des cartes à mémoire simple, représentant la première génération de la carte à puce [62]. Ces cartes ne contiennent qu'une zone mémoire et le minimum de logique nécessaire à leur fonctionnement [63]. La seconde étant celle des cartes logique à mémoire protégée et sont une évolution des premières. Elles associent une mémoire accessible en lecture et en écriture dans certaines zones et la logique nécessaire à l'exécution d'automates simples. Ces deux types de cartes sont le plus souvent utilisés dans les domaines des transports, des cartes prépayées et du cinéma [62].

Les **cartes à microprocesseur**, pour leur part, sont de véritables mini-ordinateurs. Ces cartes disposent de la même structure que ce dernier. Dès lors, le microprocesseur qu'elles possèdent peut effectuer des opérations cryptographiques complexes. Elles sont aussi dotées d'une unité centrale, d'une mémoire morte programmable et électriquement effaçable (EEPROM), d'une mémoire vive, d'une interface d'entrées et de sorties, ainsi que de toutes les logiques nécessaires à leurs fonctionnements [60]. Ces cartes sont utilisées dans les domaines bancaires, dans la téléphonie mobile et la santé. [62].

Enfin, concernant les **cartes sans contact**, elles sont identiques aux cartes à microprocesseur presqu'en tout point, excepté que contrairement à ces dernières, elles sont munies d'une antenne leur permettant de communiquer à distance avec un lecteur de carte [57]. Ces cartes sont de la gamme des Radio Frequency Identification Devices (RFID) et sont découpées en trois catégories [4.1]. D'une part, les cartes à basses fréquences, qui sont celles dont la portée est de quelques millimètres.

Elles sont suivies des cartes à hautes fréquences, qui sont d'une portée de quelques centimètres à quelques décimètres. Enfin viennent les cartes à ultra-haute fréquences, ayant une portée de quelques mètres. Ces cartes sont utilisées dans des domaines identiques aux cartes à puce disposant de microprocesseur.

Comme nous le verrons tantôt, ces différents types de cartes sont soumis à des normes de sécurisation pendant leurs phases de production et d'utilisation.

4.3. Sécurisation des cartes lors de la production et de l'utilisation.

La sécurisation pendant la **production** et l'**utilisation** est primordiale pour fiabiliser les cartes à puce. Elles ont pour but d'assurer principalement l'intégrité, l'authenticité et la non-répudiation des données transmises.

Effectivement, au cours de sa conception, la carte doit être conforme aux attentes du commanditaire définies dans le cahier de charges. Selon la circulaire N°1083/SGDN/DCSSI/SDR de la Direction Centrale de la Sécurisation des Systèmes d'Informations (DCSSI) du secrétariat général de la défense nationale française, parue le 15 mai 2006, la personnalisation et la distribution des cartes à puce doivent avoir lieu en trois étapes contenant sept phases soit [64] :

Étape 1 : Développement et fabrication du produit. Cette étape contient les trois premières phases de production, la phase 1 étant réservée à l'élaboration de l'application. La seconde quant à elle est consacrée au développement du microcircuit et de son logiciel dédié, ainsi qu'à la construction de la base de données du produit et à la fabrication du masque. Enfin, la troisième sert à la fabrication dudit microcircuit et aux tests et pré-personnalisation.

Étape 2 : Administration du produit. Celle-ci contient les trois autres phases de la production. C'est ainsi que la quatrième sert à la mise en micromodule et à des tests, pendant que la suivante permet l'encartage et l'effectuation de tests. La sixième phase, pour sa part, voit la personnalisation du produit qui sera aussi suivie de tests.

Étape 3 : Utilisation. Cet ultime stade consiste à l'utilisation concrète du produit jusqu'à sa fin de vie.

Chacune de ces phases a pour objectif d'assurer un niveau de sécurité jugé satisfaisant par rapport au cahier de charges. Elles doivent veiller à ce que lors des tests, les données ne puissent être accessibles que par le destinataire [44].

La figure 4.1. ci-dessous illustre bien nos précédents propos.

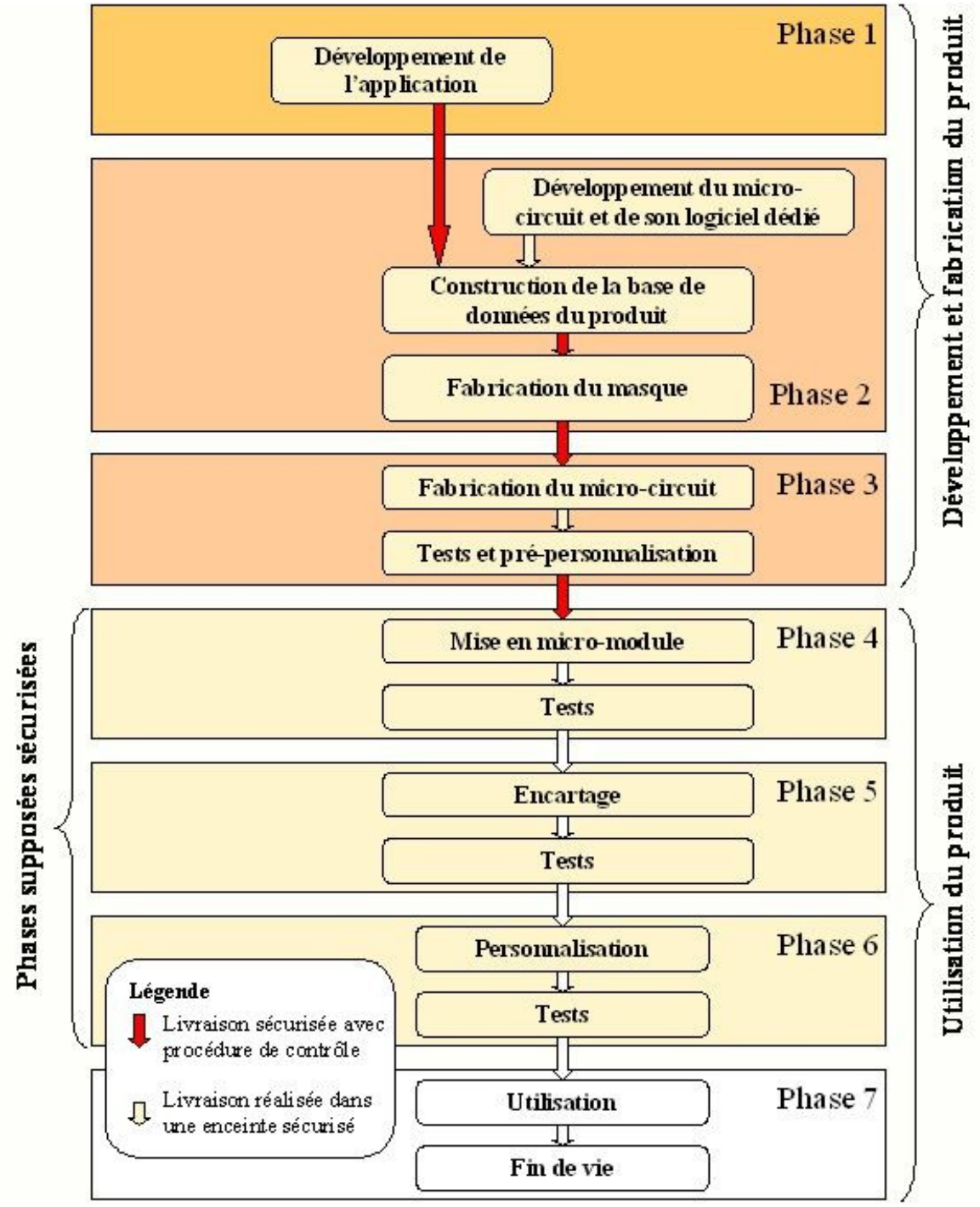

Figure 4.1. Cycle de vie d'une carte à puce. [64].

Outre les règles auxquelles elles sont soumises en tant que cartes à puce, les **cartes de paiement à puce** sont régies par la norme ISO 10102. C'est alors que, le support en pvc devra contenir les informations relatives à l'émetteur et à l'individualisation de l'utilisateur.

Ainsi, généralement le recto de la carte contient non seulement la puce à microprocesseur assurant la communication avec le terminal, mais aussi le nom et le logo de l'institution émettrice de la carte. Il contient également le numéro de la carte ainsi que sa date de validité, le nom du titulaire (dans le cas de la carte de crédit) et un hologramme destiné à rendre la carte infalsifiable. Tandis que le verso contient plutôt les logos des consortiums de paiements partenaires, la zone de signature et le numéro de téléphone de l'organisme émetteur.

De plus, les normes ISO 8732 et ANSI X9.17 déterminent la gestion des clés cryptographiques [4.2]. Les spécifications qu'elles éditent, régulent les cartes de paiement dans le cadre d'une utilisation internationale sécuritaire [44]. De surcroît, la sécurité des communications lors des transactions nécessitant l'utilisation des cartes de paiement à puce sont régies par les spécifications de l'EMV expliquées ci-après.

4.4. Normes EMV pour les cartes de paiement.

La structure sécuritaire des cartes de paiement à puce lors des transactions et leur interopérabilité avec les TPE obéissent aux normes EMV, le référentiel dans le domaine. Leur importance est d'autant plus soulignée par Visa Canada qui soutient que : « les normes EMV définissent les attributs critiques que doivent posséder les cartes à puce et leurs terminaux de lecture. Ces normes internationales, développées par Europay, MasterCard et Visa veillent à ce que les titulaires de carte, partout dans le monde, profitent de cette innovation en matière de sécurité. Grâce à la technologie de la carte à puce et à la norme EMV, vous pouvez vous attendre à une sécurité et à une protection contre la fraude améliorées, à une vitesse de traitement des transactions accrue, ainsi qu'à une commodité et une convivialité de la carte» [4.3]. En somme, EMV a développé plusieurs mécanismes dont ceux permettant d'authentifier la carte et son utilisateur dans le but d'assurer l'intégrité et la non-répudiation des données.

4.4.1. Authentification de la carte.

Authentifier la carte prévient contre la contrefaçon, identifie les fausses cartes et le cas échéant bloque la transaction. Elle peut avoir lieu online ou offline, ou encore être une combinaison de ces deux cas de figure [65]. Toutefois, l'authentification online est exceptionnelle car elle ne s'effectue que pour des transactions mettant en relation des forts montants ou des Distributeurs Automatiques de Billets (DAB). Il est donc préférable de ne se limiter qu'à la description des trois méthodes EMV que sont les authentifications statique, dynamique et combinée des données du point de vue de l'authentification offline. Lors de ces différentes procédures, c'est le terminal qui initie la conversation et détecte le type d'authentification compatible avec la carte [66].

C'est de cette façon que, nous commencerons par le principe de l'**Authentification Statique des Données** plus connue sous son acronyme anglais **SDA**. Celle-ci repose sur la vérification par une autorité de certification des signatures des données (nom, prénom, numéro de compte bancaire) et de la clé publique, signatures faites par l'émetteur de la carte. Ces données sont introduites dans la carte lors de sa production [65, 67]. Par conséquent, lors d'une transaction, le terminal s'assure de l'intégrité de la carte en les vérifiant [68, 4.4]. La génération de la signature se fait en utilisant la fonction de hachage SHA-1 et une certification RSA de la clé secrète. L'on se sert d'un paradigme hach-et-signe et d'un chiffrement RSA sur la clé publique pour vérifier la signature ainsi obtenue.

Néanmoins, le protocole SDA est vulnérable aux clonages des cartes, en ce sens que le terminal est incapable de détecter une carte clonée lors de l'authentification offline [65].

La figure 4.2. ci-dessous est une illustration de SDA.

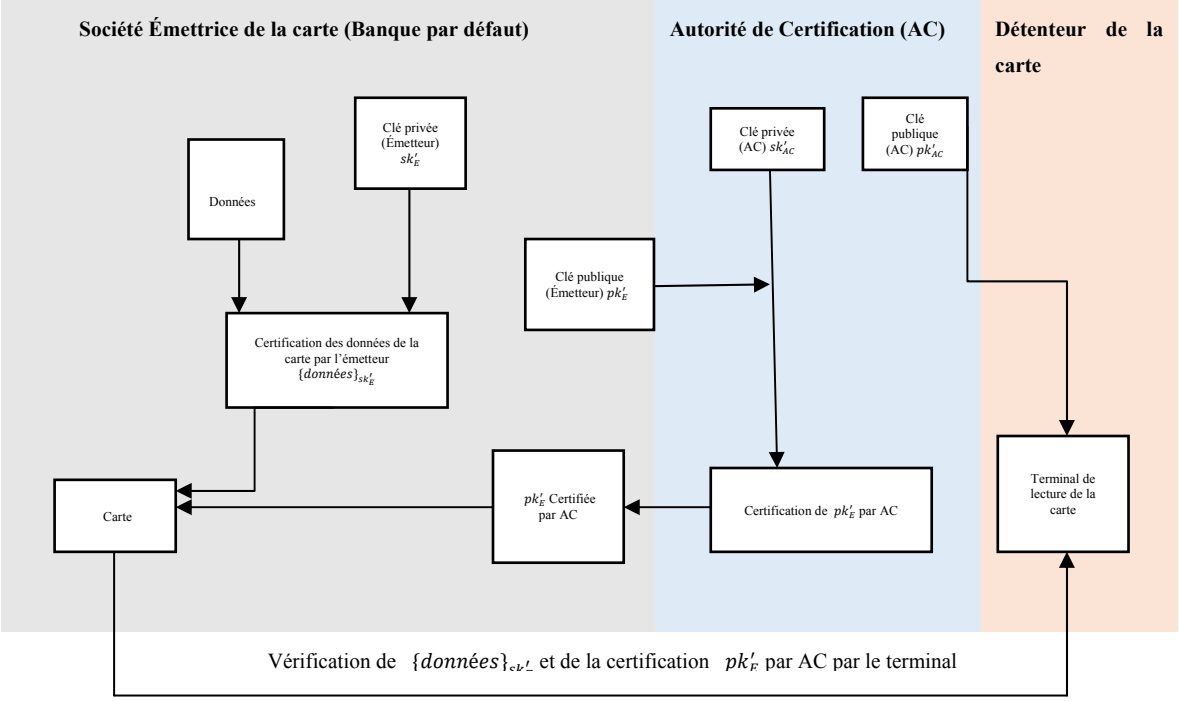

Figure 4.2. Authentification Statique des Données offline (modifié) [4.4]**.**

Le principe de l'**Authentification Dynamique des Données** ou **DDA**, acronyme de sa traduction anglaise, est presque similaire à celui du SDA à la seule différence que ce dernier contient une paire de clés RSA pour chaque carte et génère un cryptogramme unique à chaque transaction en faisant intervenir un nombre aléatoire [65]. À sa production, sont introduites dans la carte la paire de clés RSA (pk'_c ,sk'_c), les données (nom du porteur, numéro de la carte, date de validité etc.) et la valeur de la signature de ces données $\{données\}_{sk'_E}$ associée au certificat la clé publique de la carte $\{pk'_c\}_{sk'_E}$. Elles sont signées par l'organisme émetteur de la carte. Il y a également un autre certificat signé par une autorité de certification contenant la clé publique de l'organisme émetteur de la carte $\{pk'_E\}_{sk'_{AC}}$. Hormis la signature de la clé privée sk'_c située dans une zone inaccessible de la carte, toutes les autres informations sont publiques. Le terminal, quant à lui, dispose de la clé publique pk'_{AC} de l'autorité de certification [68].

Soient alors, *C* la carte, *T* le terminal et N_T un nombre aléatoire, le protocole d'authentification DDA se déroulera comme les cinq étapes suivantes le montre [4.4, 69] à savoir :

1- Lors de l'introduction de *C* dans *T,* ce dernier demande à *C* de s'authentifier;

2- *C* fournit alors à *T* les informations contenues dans sa partie publique qui est le couple *données,*$\{données\}_{sk'_E}$, $\{pk_c\}_{sk'_E}$, $\{pk_E\}_{sk'_{AC}}$;

3- *T* génère ensuite une valeur aléatoire N_T et l'envoie à *C* ;

4- *C* produit et signe C_T et signe également N_T avec sa clé privée avant d'envoyer à *T* $\{N_T\}_{sk'_c} = N$.

5- *T* vérifie de ce fait $\{pk'_E\}_{sk'_{AC}}$avec la clé publique pk'_{AC} de l'autorité de certification et vérifie aussi $\{pk'_c\}_{sk'_E}$ avec la clé publique de la banque pk'_E. Par ailleurs, il authentifie *N* avec la clé publique de la carte pk'_c, et s'il obtient $[N]_{pk'_c} = N_T$ alors *T* a la garantie qu'il communique bien avec *C*.

La figure 4.3. schématise l'authentification DDA.

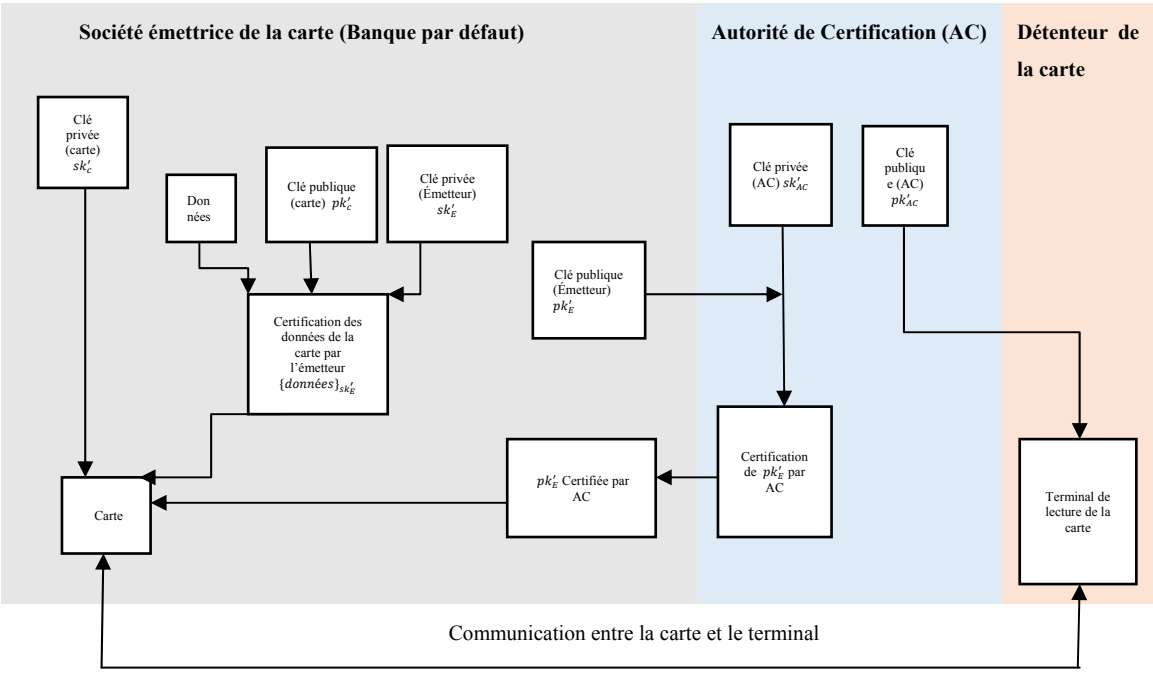

Figure 4.3. Authentification Dynamique des Données de la carte offline (modifié). [4.4]

Quant à l'**Authentification Combinée des Données** ou en anglais Combined Data Authentification (**CDA**) c'est une version plus sécurisée de la DDA. Elle associe une signature dynamique à un Cryptogramme d'Application[10] (CA) [67].
Ce type d'authentification est en mesure de détecter une attaque de l'homme du milieu par la vérification de la signature sur le CA généré par la carte au niveau du terminal, ce dont DDA est incapable. De plus CDA est plus rapide lors des transactions [4.4].

4.4.2. Authentification du détenteur de la carte.

Le processus d'authentification du détenteur de la carte est une mesure visant à s'assurer que l'utilisateur en est bien le propriétaire. Il dépend de la communication avec la carte initiée par le terminal et peut s'effectuer selon les huit méthodes qui suivent [4.5, 4.6] :

1- **Vérification ne requérant aucun élément d'authentification du détenteur.** Dans ce cas le détenteur de la carte se doit juste de passer sa carte devant le lecteur.
2- **Vérification par signature.** Ici, il est à la charge du commerçant de demander au client de signer une copie du reçu de l'achat.
3- **Vérification du NIP online.** Cette méthode consiste à demander au client de saisir son NIP, qui sera par la suite chiffré par le terminal et transmis à l'émetteur de la carte pour vérification.
4- **Vérification du NIP Chiffré offline.** Ici, la carte vérifie le NIP chiffré qui lui est transmis par le terminal.
5- **Vérification du NIP clair offline.** Au cours de ce processus, la carte vérifie le NIP non-chiffré qui lui est transmis par le terminal.
6- **Vérification du NIP clair offline et vérification par signature.** Cette méthode est tout simplement la combinaison de la vérification du NIP en clair offline et de la méthode par vérification de signature.
7- **Vérification du NIP chiffré offline et vérification par signature.** Cette méthode est la combinaison de la vérification du NIP chiffré en mode offline et de la méthode par vérification de signature.

[10] https://www.level2kernel.com/emv-glossary.html.

8- **Échec de la procédure de vérification**. Dans ce cas de figure, le terminal est poussé à déterminer le type de vérification du détenteur.

4.4.3. Intégrité et non-répudiation des données.

Pour contrer la répudiation des transactions et garantir leur intégrité, les standards EMV s'assurent que lors d'une transaction, un cryptogramme est généré. Il s'agit d'un CAM calculé par la carte à l'aide d'un triple DES sur les données (type de transaction, date, heure...) qui scelle le résultat de la transaction et prouve l'effectivité de ladite transaction [4.4]. C'est une méthode couramment utilisée concernant les cartes de débit et de crédit dont nous discuterons subséquemment.

4.5. Cartes de débit et de crédit.

Le fonctionnement conventionnel des cartes bancaires introduit l'analyse prochaine et ce de façon indépendante des cartes de débit et de crédit. Celle-ci aura pour base des critères tels que la confiance des utilisateurs, la protection de la vie privée et l'anonymat.

4.5.1. Fonctionnement conventionnel de paiement par carte bancaire.

Lors d'un achat par carte de débit ou de crédit, l'argent est transféré par les institutions financières qui se chargent d'ajuster les comptes respectifs des acteurs de la transaction. La procédure est généralement la suivante.

Tout d'abord, le client introduit sa carte dans le TPE pour régler son achat (1), initialisant ainsi la communication avec la banque du vendeur dans l'optique d'une vérification de sa faisabilité (2). C'est alors que, la banque du vendeur communique avec celle du client pour s'assurer que le compte de ce dernier peut couvrir le montant de l'achat (3). Si tel est le cas, la banque du client se charge de transférer le montant équivalent à l'achat dans le compte du vendeur (4) ; Sinon, elle envoie un message de non-autorisation à la banque du commerçant. Cette dernière transmet au commerçant via le TPE la confirmation du paiement ou son refus (5). Le commerçant peut ainsi remettre ou pas au client l'objet de l'achat. Nos dires sont résumés par la figure 4.4.

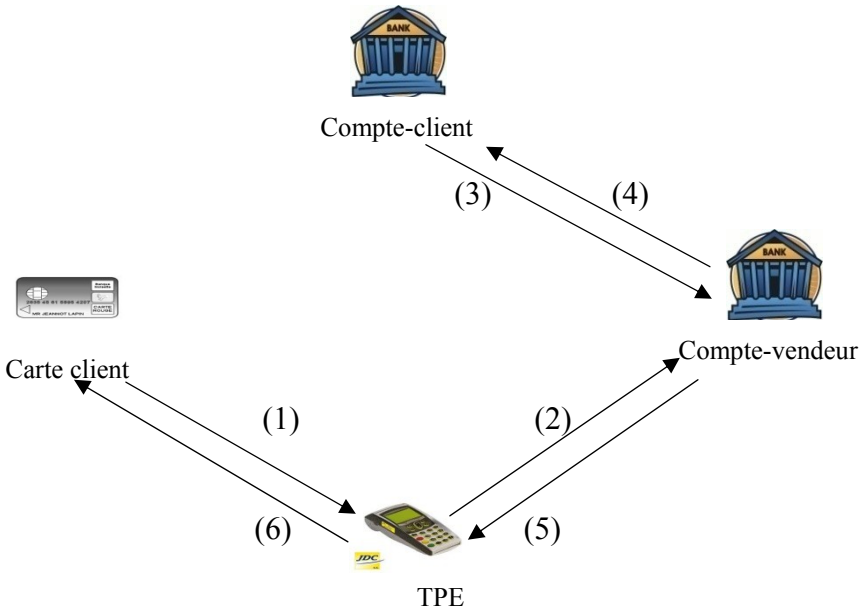

Figure 4.4. Fonctionnement conventionnel de paiement par carte [14].

4.5.3. Analyse de la carte de débit.

Les cartes de débit sont émises par les banques pour leurs clients et sont directement rattachées à leurs comptes chèque si bien qu'elles constituent un moyen de paiement avec accès direct à ces comptes bancaires [4.8]. En conséquence, pour acquérir la **confiance des utilisateurs**, les organismes émetteurs de carte de débit ont mis un accent sur leur sécurité. Au canada par exemple, les cartes à puce remplacent peu à peu celles à bande magnétique ayant plus de failles de sécurité [4.9].

La mise en place de ces différentes normes de sécurisation a permis de réduire considérablement les fraudes, leur coût passant ainsi de cent quarante-deux millions de dollars (142 000 000 CAD) en 2009 à vingt-neuf millions (29 000 000 CAD) en 2013. De surcroît, le taux assez bas de clonage de la carte se chiffrant à 0,5% contribue à rassurer les clients [4.10]. De plus, le fait que les institutions financières canadiennes soient juridiquement contraintes de protéger les informations qu'elles collectent auprès de leurs adhérents, et ce en vertu des lois fédérales et provinciales sur la protection de la vie privée et la divulgation des informations, elles **protègent la vie privée** de ces derniers [1.13].

Cependant, les cartes de débit ne sont pas **anonymes**, puisque liées aux comptes bancaires de leurs utilisateurs contenant toutes les informations permettant de les identifier [4.8].

En effet, les institutions financières sont dans l'obligation d'identifier leurs potentiels clients avant de leur permettre de pouvoir ouvrir un compte en vertu de l'article 448.1 de la loi canadienne sur les banques [4.11].

Toutefois, les transactions par cartes de débit respectent les propriétés **ACID**. Elles sont atomiques, parce que complétées entièrement ou pas du tout. Elles sont tout aussi cohérentes, en ce sens que, le montant débité du compte de l'acheteur est celui qui crédite le compte du vendeur. De plus elles sont isolées car deux transactions peuvent être traitées de façon indépendante. Enfin, elles sont durables puisque toutes les transactions sont conservées dans un registre (historique de transactions). [45]

En outre, les cartes de débit, peuvent être considérées comme étant **divisible** car offrant la possibilité d'effectuer des achats à des montants différents.

En revanche, de nombreuses **menaces** pèsent sur la carte de débit. Le clonage étant la principale. À cela, il est envisageable de rajouter les vols [4.10]. Pour prévenir ces éventuels périls, l'association Interac conseille à ses utilisateurs de protéger leur NIP, d'éviter d'utiliser la carte à bande magnétique quand il est possible d'utiliser la carte à puce [4.9].

En guise de conclusion, nous pouvons dire que la carte de débit en plus de pouvoir être utilisée à l'internationale et de renforcer la sécurité et la rapidité des transactions, présente de nombreux avantages en particulier la facilité de paiement qu'elle permet tout en conservant un historique des achats effectués. Elle utilise l'authentification par NIP qui endigue les risques en cas de perte ou de vol [18]. D'un autre côté, elle a aussi des inconvénients. En effet, un paiement ne peut être réalisé sans disposer des fonds nécessaires (paiement à crédit). En plus, elle n'est pas anonyme et ne permet pas de paiement à des particuliers [18]. Par ailleurs, lorsqu'il y a dépassement du nombre mensuel permis de transactions ou au cours de l'utilisation d'un DAB n'appartenant pas à l'institution financière dont l'utilisateur est initialement client, des frais supplémentaires se rajoutent à la facture [4.7].

4.5.4. Analyse de la carte de crédit.

Les cartes de crédit sont émises par des organismes privés spécialisés tels que les banques et les institutions de crédit. Elles permettent d'effectuer des paiements à crédit via une avance de fond faite par l'organisme émetteur qu'il faut régler de façon mensuelle [14]. Tout comme pour la carte de débit, nous effectuerons aussi une analyse de la carte de crédit.

Ainsi, les sociétés émettrices de cartes de crédit ont compris que pour obtenir la **confiance des utilisateurs**, la priorité devait être portée sur la sécurité. Pour cela, les cartes de crédit sont soumises à différentes normes évoquées plus haut. Outre ces mesures, ces sociétés ont commencé à mettre en place des systèmes d'authentification lors des achats faits sur l'internet. Dorénavant, excepté les informations « traditionnelles » rentrées lors de ces achats, il faut en plus saisir un mot de passe pour valider la transaction. Les exemples les plus marquants sont le *verified* by Visa et le *SecureCode* de Mastercard. [4.12, 4.13]

De plus, au même titre que pour la carte de débit, les utilisateurs de la carte de crédit sont en droit d'attendre des institutions émettrices de ces cartes qu'elles protègent leurs informations en vertu des lois fédérales et provinciales dans le cadre de **la protection de la vie privée** [1.13].

Néanmoins, les transactions par carte de crédit ne sont pas **anonymes**. Les organismes émetteurs associent à chaque carte de crédit l'identité de son utilisateur. En effet, ils sont possession de toutes les informations permettant d'identifier un individu [45]. Par contre, lors d'achat sur internet, une certaine forme d'anonymat peut être acquise en payant à travers des plateformes d'anonymisation telle qu'Allopass [4.14].

Outre cela, les transactions par carte de crédit n'obéissent pas à toutes les propriétés **ACID**. En effet, elles ne peuvent être qualifiées d'atomiques, puisque d'autres transactions peuvent être faites sans que la précédente ne soit complétée. Elles sont, toutefois, cohérentes car le compte du vendeur est crédité du débit fait sur le compte de l'acheteur et ce transfert correspond au prix de la transaction. Elles ne sont pas isolées parce que, dans certains cas

le vendeur obtient certains blocs sur le crédit de l'utilisateur qui n'est pas toujours rapidement effacés ce qui peut dans des cas conduire à l'échec de l'isolation [45].
Par contre, on peut les qualifier durable, toutes les transactions étant contenues dans un historique.
Par ailleurs, tout comme pour les cartes de débit, les paiements par carte de crédit sont **divisibles** car, des achats de divers montants peuvent être effectués.
En dépit de cela, de nombreuses **menaces** pèsent sur la carte de crédit. En effet, les différentes fraudes que peuvent subir cette dernière, le vol ou la perte d'une carte de crédit, le clonage de la carte, l'hameçonnage par téléphone ou par internet sont tant de menaces identifiées par la Gendarmerie Royale du Canada (GRC) [4.15].
En somme, en plus de renforcer la sécurité et la rapidité des transactions, la carte de crédit à de nombreux avantages. Effectivement, elle procure une protection contre la fraude et est de plus acceptée dans plus de cent cinquante (150) pays et des millions de commerces à travers le monde. La responsabilité zéro pour les utilisateurs en cas de fraude en sont d'autres mis en avant par l'Association des Banquiers Canadiens (ABC) [4.16]. Malheureusement, elle comporte également des désavantages. L'union des Consommateurs du Canada (UCC) fait du coût lié à son utilisation, le véritable inconvénient de la carte de crédit [14]. À cela, on peut ajouter le fait que la carte de crédit ne confère aucun anonymat.

En définitive, retenons de ce chapitre qu'il a d'abord introduit les cartes à puce à travers un historique, qu'il a ensuite explicité leurs caractéristiques et les normes auxquelles elles sont soumises. D'un autre côté, les deux principaux types de cartes de paiement à puce que sont la carte de débit et la carte de crédit ont été analysés.

Chapitre 5. Pistes et solutions.

Les chapitres précédents nous ont permis d'analyser et de comprendre divers moyens de paiement. Il parait évident que le moyen de paiement idéal serait celui procurerait un anonymat et assurerait le respect de la vie privée tout en demeurant sûr ; Mais aussi d'une certaine manière respecterait les propriétés ACID, serait divisible et en conformité avec les attentes des banques.

Malheureusement, le constat est que l'anonymat est le critère faisant le plus défaut à la majorité. Alors, pour essayer de l'obtenir nous avons entrepris de proposer d'une part un système qui permettrait de rendre les cartes de débit anonymes et qui renforcerait par la même occasion la protection de la vie privée. La monnaie fiduciaire et les chèques pouvant être difficilement plus améliorés qu'ils ne le sont déjà, nous tenons à préciser que nous avons décidé d'un côté de présenter une approche qui permettrait d'obtenir l'anonymat des comptes bancaires et par conséquent pour les cartes de débit également. En effet, nous nous sommes rendu compte que les cartes de débit procuraient déjà une certaine sécurité ainsi qu'une protection de la vie privée acceptable, tout en étant respectant les autres exigences susmentionnées. Toutefois le seul bémol concernant ce moyen de paiement était l'inexistence de l'anonymat. Effectivement, étant obligatoirement liées à un compte bancaire (épargne ou chèque), les cartes de débit sont par essence tout sauf anonymes. Les banques au sein desquels sont domiciliés lesdits comptes ont accès s'ils le désirent aux activités des propriétaires, c'est-à-dire l'endroit où ceux-ci se trouvent, le montant de l'achat effectué ou encore le ou les articles qui font l'objet du paiement.

Cependant, il était tout aussi intéressant de développer une approche inspirée d'un système de jetons, en référence aux autres moyens de paiements électroniques que sont DigiCash et bitcoin. Couplée à la technologie des cartes à puce, cet autre système implémenté sera axé sur une technologie utilisant des jetons inspirée de celle des cartes opus de la STM. La composition des jetons des cartes à puce sera, elle, calquée en partie du fonctionnement de DigiCash et de bitcoin, tandis que la sécurité de ce second système sera la même que celle mise en place relativement aux cartes de débit.

Une combinaison de ces deux propositions sera développée à leur suite, en vue d'engendrer un système hybride qui en réduirait les lacunes.

5.1. Première approche : Comptes bancaires anonymes.

Cette démarche sera graduellement bâtie autour des éléments constitutifs permettant d'aboutir aux différents protocoles. De fait, dans un premier temps, il serait pertinent d'étudier la position juridique canadienne face aux comptes bancaires anonymes; Ensuite, nombre d'éléments tels que le protocole DDA, ainsi que l'attribution des pseudonymes, l'utilisation des autorités de certification, la limitation des montants ou encore la transférabilité se doivent d'être évoqués, avant qu'une conclusion ne vienne parachever l'analyse de ce système.

5.1.1. Loi canadienne sur l'ouverture des comptes bancaires.

La loi canadienne ne permet pas l'ouverture de comptes bancaires anonymes. En effet, l'article 448.1 du règlement relatif à l'accès aux services bancaires de base, fait formellement état que certaines informations sont indispensables à l'ouverture d'un compte. Il exige notamment que le demandeur fournisse:

- d'une part, deux pièces permettant clairement de l'identifier. Ces documents pouvant être un permis de conduire, un passeport, un certificat de citoyenneté canadienne ou de naturalisation etc.;
- et d'autre part, de façon verbale ou écrite, son nom, sa date de naissance, son adresse civile et son occupation. Ces renseignements sont prévus à la partie c de l'annexe dudit article.

Après vérification, la banque se réserve le droit d'accéder à la demande du requérant ou non. Une des raisons possibles de refus serait le fait que des soupçons planent sur la véracité des informations fournies [5.1].
De ce fait, le système proposé ici est par essence 'hors-la-loi' sauf si changement il y a.

5.1.2. Retour sur le protocole DDA d'authentification offline des cartes.

Nous aurions tout aussi bien pu choisir les protocoles SDA ou CDA pour nous illustrer mais, le choix du protocole DDA (dans ces deux premières phases) s'est naturellement imposé car des trois évoqués il est le plus utilisé.

Soient alors *C* la carte et *T* le terminal, le protocole d'authentification DDA, dans ses deux premières phases, se déroule ainsi :

1- Lors de l'introduction de *C* dans *T,* il demande à *C* de s'authentifier ;

2- *C* fournit à *T* les informations contenues dans sa partie publique que sont : *données,*$\{données\}_{sk'_E}$, $\{pk_c\}_{sk'_E}$, $\{pk_E\}_{sk'_{AC}}$.

Après observation de ce protocole, il est aisé de remarqué que les informations contenues dans le couple (*données,*$\{données\}_{sk'_E}$) fournies lors de l'ouverture d'un compte permettant d'identifier le détenteur de la carte et introduites dans la carte sont transmises au cours de la phase 2 de DDA. De ce fait, le constat est tel que pour anonymiser les comptes bancaires et les cartes associées, il faudrait se focaliser sur les données tout en permettant si besoin est d'identifier le détenteur du compte.

5.1.3. Utilisation des pseudonymes.

L'utilisation des pseudonymes uniques et distincts en lieu et place des informations (Nom, prénom(s), adresse…) fournies lors de l'ouverture d'un compte bancaire et introduites dans la carte sous le couple (*données,*$\{données\}_{sk'_E}$) servirait à rendre ces dernières anonymes.
En effet, si cet ensemble d'informations identifiant une certaine Alice est remplacé par un pseudonyme comme 'Bob', l'on ne dispose plus dès lors d'aucun moyen pour savoir que Bob est en fait Alice, sauf si l'on est l'attributaire dudit pseudonyme.

Cela deviendrait encore plus difficile à déterminer si 'Bob' à son tour empruntait un autre pseudonyme et se faisait désormais appeler César. Et ainsi de suite, le niveau de complexité allant croissant, un pseudonyme pour en cacher un autre.

Il faut cependant noter que l'utilisation de pseudonymes sans contrôle peut s'avérer dangereuse. Effectivement, si d'une part les utilisateurs n'avaient qu'à les communiquer

aux banques sans plus d'informations d'identification, des fraudes massives sans possibilité de reconnaître les malfaiteurs seraient récurrentes. D'autre part, s'ils sont attribués par les banques après vérification des informations, celles-ci sauraient qui se cache derrière chaque pseudonyme ce qui de facto annulerait l'anonymat des comptes.

Pour endiguer ces problèmes, l'utilisation d'un ou plusieurs tiers de confiance (Autorité de certification) qui vérifieraient les informations du demandeur et s'assureraient que le pseudonyme choisit par ce dernier est valide (non utilisé) est la solution la plus probable. Il s'agirait d'une sécurité garantie pour la banque tout en permettant au client de préserver son anonymat.

Pour rappel, le Larousse définit un pseudonyme comme un nom d'emprunt sous lequel se cache l'identité réelle de la personne qui l'utilise pour une activité quelconque [1.1] . Cette activité quelconque étant ici l'ouverture d'un compte.

5.1.4. Autorités de certification.

La section précédente a notifié que l'utilisation d'un ou plusieurs tiers de confiance permettrait de rassurer les banques et leurs clients. C'est ainsi que dans cette approche sur les comptes bancaires anonymes, le choix s'est porté sur l'utilisation de deux types d'autorité de certifications: une autorité de vérification d'autorisation bancaire (AVAB) et une autorité d'anonymisation (AA). Il s'agira d'en évoquer les rôles, les informations qu'elles détiendraient et la façon dont elles en disposeraient.

5.1.4.1. Autorité de vérification d'autorisation bancaire (AVAB).

L'AVAB est la première autorité de certification à qui il faudrait se référer pour ouvrir un compte bancaire anonyme. Elle aura pour rôle premier de vérifier la validité des informations fournies par le client. Par la suite, elle devra associer ces informations au pseudonyme valide choisit par ce dernier.

Après avoir complété ses deux premiers rôles, l'AVAB fournira un certificat du pseudonyme au client. Ensuite, pour des besoins de communication futurs entre le client et l'autorité d'anonymisation, l'AVAB rangera ces informations dans une table à deux zones : une zone publique qui contiendra le pseudonyme du client tandis qu'une autre

zone, celle-là privée, aura les informations permettant d'identifier le client. Le tableau 5.1. suivant nous donne un aperçu de la disposition des données dans la table de l'AVAB.

Tableau 5.1. Exemple de données contenues dans la table de l'AVAB.

Informations publiques	Informations privées
Pseudonyme : Bob	Nom et adresse civique : Alice Jules, 3300 Avenue du capitole #10, Montréal, H1L 2N0 (QC), Canada

5.1.4.2. Autorité d'anonymisation (AA).

L'AA est la seconde autorité de certification à laquelle il faudra s'adresser lors de l'ouverture d'un compte bancaire anonyme. Elle aura pour rôle de vérifier que le pseudonyme communiqué par le client existe bel et bien et qu'il a déjà été certifié par l'AVAB. Elle devra ensuite lui en associer un autre dont elle aura au préalable vérifié la disponibilité. Après validation, l'AA rangera le nouveau pseudonyme associé à celui de l'AVAB dans la zone privée de sa table, tout en le publiant dans sa zone publique. Certes, il sera difficile de prédire le nombre d'AA à utiliser, mais il faut noter qu'il sera possible d'en faire appel à plusieurs.

Néanmoins, il faudrait trouver un moyen dont la banque se servirait pour vérifier que le pseudonyme fournit par le client provient bien de l'AA, et ainsi lui permettre de remettre directement à ce dernier sa carte bancaire sans qu'il n'ait à divulguer d'informations pouvant l'identifier. Pour cela, le système de gestion de mots de passe fonctionnant comme sous le système d'exploitation multitâches et multi-utilisateurs, Unix, semble le plus approprié.

Soient donc *f* une fonction à sens unique, *M* le mot de passe et *s* un nombre aléatoire appelé sel[11], différent pour tous les utilisateurs. Ainsi, lors de la création du mot de passe, le serveur calcule l'empreinte *f(M, s)* de *M* associée à *s* et la stocke dans le fichier à côté du nom d'utilisateur. Le sel sert à distinguer l'empreinte issue d'un mot de passe identique à plusieurs personnes.

Tandis que lors d'une authentification, l'utilisateur entre le mot de passe *M'*en clair, alors que le serveur calcule *f(M', s)*, si le résultat de cette opération équivaut à *f(M, s)*, alors l'authentification en question est validée [70].

Sous Unix plusieurs fonctions de stockage de mot de passe sont utilisées aujourd'hui, dont la BSD MD5-Crypt qui est utilisée sous presque tous les Unix Open Source. Par comparaison au DES-Crypt, elle est largement plus robuste en plus d'être très lente à calculer (faisant 1000 fois appel à la fonction MD5) avec des résultats modifiés entre deux appels [4]. La lenteur du système conduira à contrer les tentatives d'attaques sur les mots de passe en évitant l'effectuation des calculs rapides pouvant conduire à leur accès.

Il faut cependant mentionner qu'ici, c'est le client qui fournira l'empreinte de son mot de passe à l'AA après l'avoir calculé à l'aide d'un logiciel, par exemple le MD5. L'AA gardera *f (M, s)* dans la zone publique de sa table aux côtés du nouveau pseudonyme choisi par l'utilisateur, tandis que dans sa zone privée elle conservera toujours le nouveau pseudonyme du client associé à celui reçu de l'AVAB comme l'illustre le tableau 5.2.

[11] Le salage, en cryptographie, est une injection de donnée(s) particulière(s), appelée(s) sel, dans une fonction de hachage, dans le but de compliquer la détermination de la donnée hachée – antécédent par la fonction de hachage – à partir de son condensé de hachage - image par la fonction de hachage .

Tableau 5.2. Exemple de données contenues dans la table de l'AA.

Informations publiques		**Informations privées**	
Pseudonymes	*f(M)*	Pseudonyme reçu de l'AA	Pseudonyme reçu de l'AVAB
Alice	$f(M_{Alice,\ s})$	Alice	Jeanny

Dans cette étude une limitation à deux autorités de certification sera faite en partant des hypothèses suivantes :

1- Les autorités de certification seront supposées honnêtes et n'étant jamais de connivence avec la banque ;
2- Les autorités de certification ne collaboreront jamais entre elles pour connaître l'identité d'un usager à partir de son pseudonyme.

Ces hypothèses permettent de garantir la confiance des utilisateurs et des banques en minimisant le risque de fraudes que peuvent subir les deux parties. Dans un objectif de renforcement de la sécurité de cette approche, une limitation du montant pouvant être déposé dans le compte est recommandé. En effet, cela permettrait d'une part au client de contrôler les pertes en cas de vol ou de piratage, et d'autre part aux banques et aux autorités gouvernementales de prévenir tout risque de blanchiment d'argent ou toute autre fraude. De plus, cette solution réduirait les procédures de levées d'anonymat demandées par l'État. Avant tout, la mise en place d'un protocole d'ouverture de compte bancaire anonyme est nécessaire.

5.1.5. Protocole d'ouverture d'un compte anonyme.

Ce procédé sera axé sur l'utilisation des pseudonymes et des autorités de certification. Sachant qu'il est possible de faire appel à plusieurs AA, pour des raisons de simplicité on n'en utilisera qu'un. Ceci étant dit, le protocole général d'ouverture d'un compte bancaire anonyme se déroulera comme suit :

1- Tout d'abord, le client fait une demande d'ouverture de compte bancaire auprès de l'AVAB. Il fournira à cette dernière les informations personnelles nécessaires à l'ouverture d'un compte associé au pseudonyme qu'il voudra utiliser. Après avoir vérifié et validé les informations et le possible pseudonyme, l'AVAB rangera ces données dans sa table. En contrepartie, le requérant recevra un certificat de son pseudonyme qui lui permettra de communiquer avec l'AA conduisant à la phase 2.

2- Ensuite, le client prendra contact avec l'AA et lui communiquera le certificat reçu de l'AVAB et le nouveau pseudonyme qu'il voudra utiliser. L'AA vérifiera le certificat à l'aide de la clé publique de l'AVAB et validera le pseudonyme avant de demander au client de fournir le hash du mot de passe qu'il aura choisi pour son pseudonyme. Elle rangera ces informations dans sa table selon la classification prédéfinie et ce nouveau pseudonyme ainsi que le hash du mot de passe seront utilisés par le client pour communiquer avec la banque.

3- Enfin, le client se présentera à la banque en utilisant le pseudonyme reçu de l'AA. Celle-ci lui demandera de s'authentifier à travers le mot de passe associé à son pseudonyme. Le client entrera le mot de passe et si le hash correspondant équivaut à celui fournit à l'AA, il est alors authentifié. La banque confirmera dès lors l'ouverture du compte au client. Et lui fournira les informations concernant son compte bancaire tout en lui remettant sa carte de débit contenant son pseudonyme, le certificat du pseudonyme, la date de validité de la carte etc.

Ce processus conclut donc les étapes de communications entre les différents acteurs lors de l'ouverture d'un compte bancaire anonyme dont nous expliquerons d'ailleurs les trois phases du fonctionnement technique à l'aide de figures.

Au préalable, il convient de signaler que certaines interactions pourraient se faire online ou physiquement. Ensuite, il faut savoir que toutes les communications online seront chiffrées en utilisant le protocole SSL[12].

Données :

Soient : U le client, $AVAB$ l'autorité de vérification, AA l'autorité d'anonymat, B la banque, pk'_{AVAB} la clé publique de $AVAB$, sk'_{AVAB} la clé privée de $AVAB$, pk'_{CAA} la clé publique de AA, sk'_{CAA} la clé privée de AA, w le premier pseudonyme de U vérifié par l'$AVAB$, sk'_E la clé privée de la banque, z le second pseudonyme de U validé par AA, et enfin $f(mdp)$ le hash du mot de passe transmis à AA par U.

Le **protocole de communication entre le client *U* et l'*AVAB*** se déroulera principalement à travers des interactions physiques. La figure 5.1. suivante en représente le déroulement.

[12] Secure Socket Layer ,
https://www.globalsign.fr/centre-information-ssl/definition-ssl.html

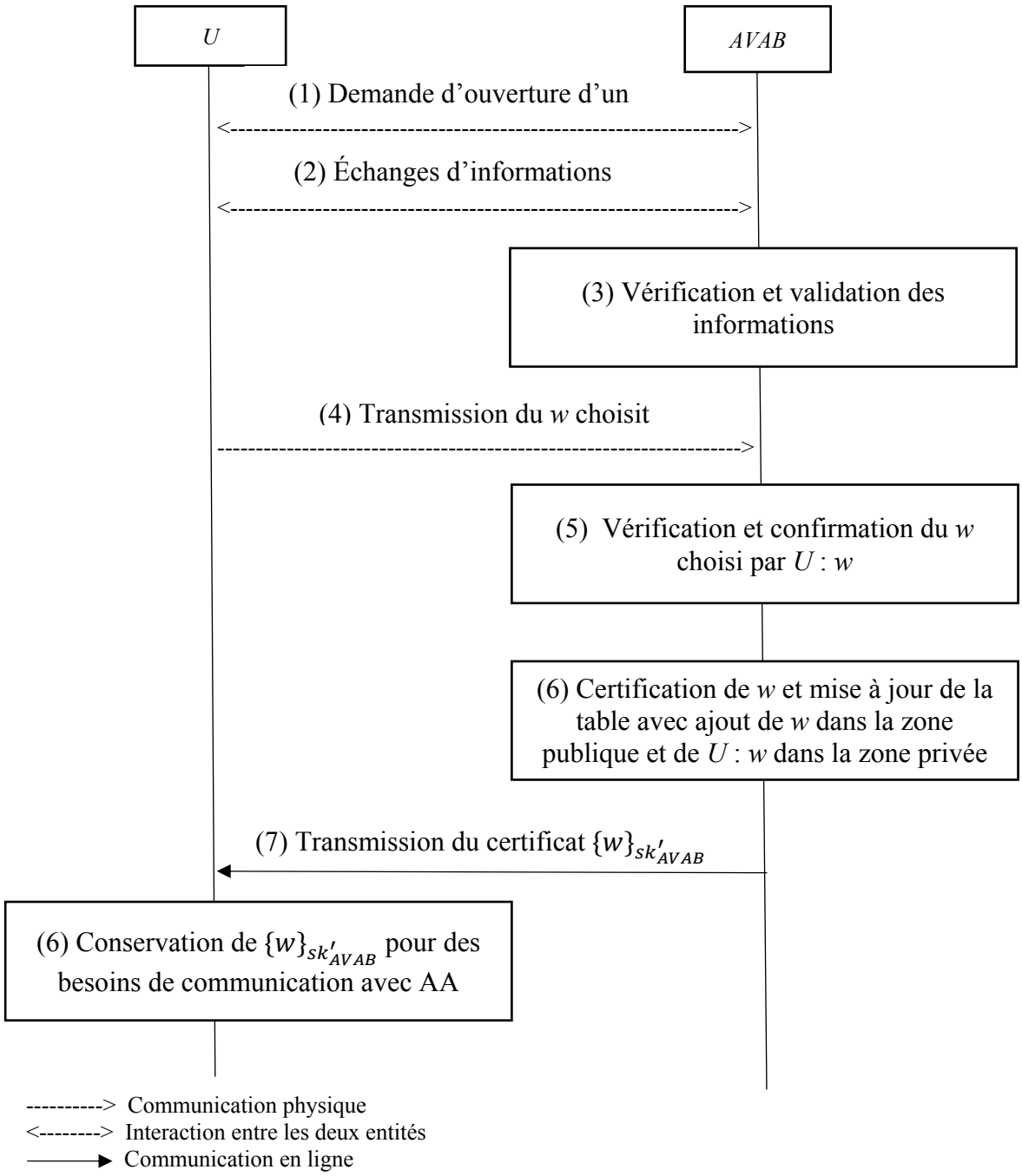

Figure 5.1. Protocole de communication entre *U et AVAB*.

Cette figure donne un aperçu des rouages de communications entre le client *U* et l'*AVAB* tout en introduisant le processus de communication entre *U* et l'*AA*.

Pour sa part, le **protocole de communication entre *U* et l'*AA*** prendra place à travers des interactions online, qui seront détaillés grâce à la figure 5.2. subséquente.

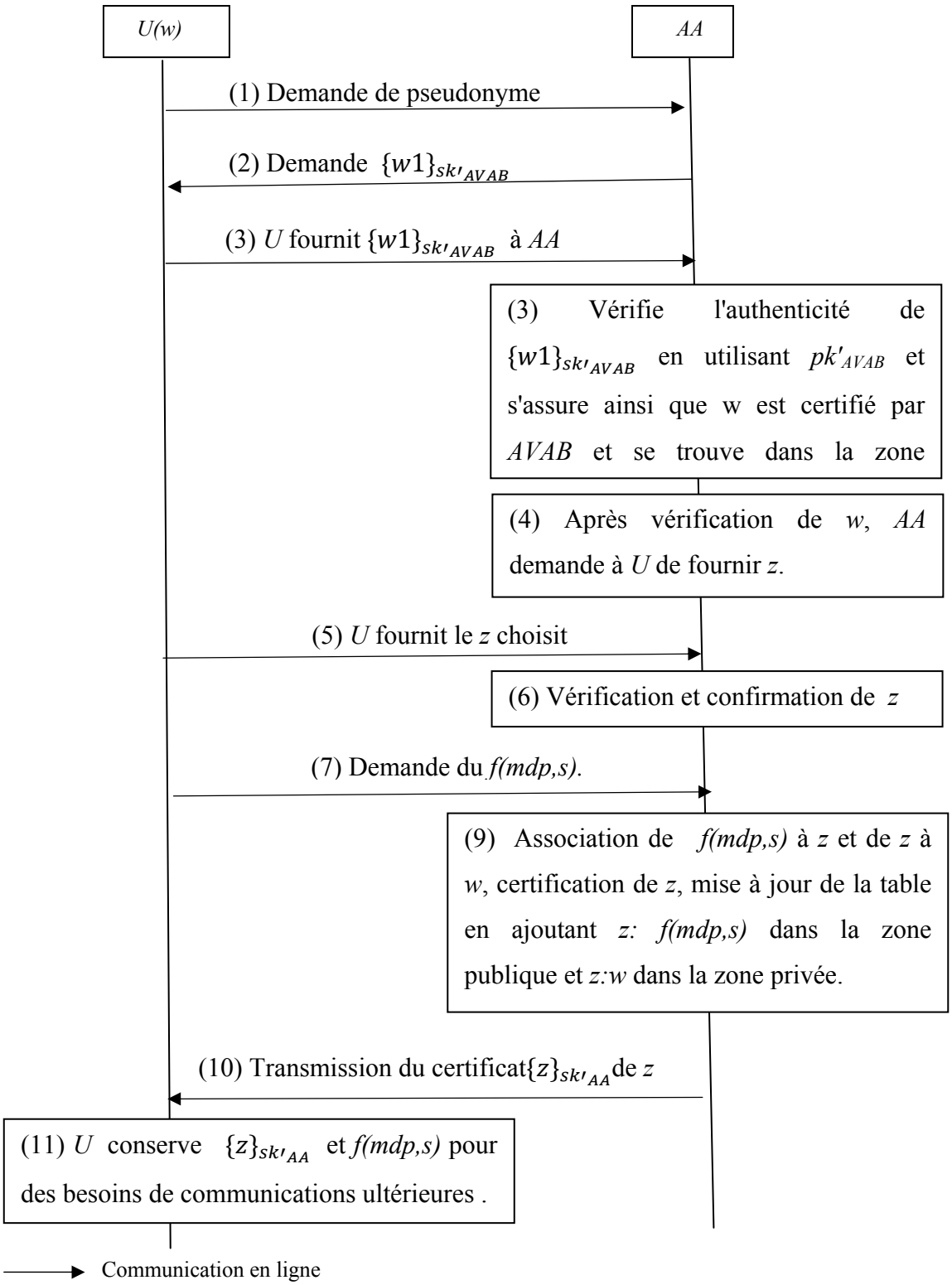

Figure 5.2. Protocole de communication entre *U* et *AA*.

Dans le cas où [illegible]t avec la *AA* suivante à l'aide de $\{z\}_{sk'_{AA}}$, sinon il userait de *f(mdp,s)* pour s'authentifier auprès de la banque au cours du protocole de communication entre *U* et *B*.

Dès lors, les **communications entre *U* et *B*** seront des interactions online parfois ponctuées de quelques actions physiques. La figure 5.3. illustre le déroulement de ce protocole.

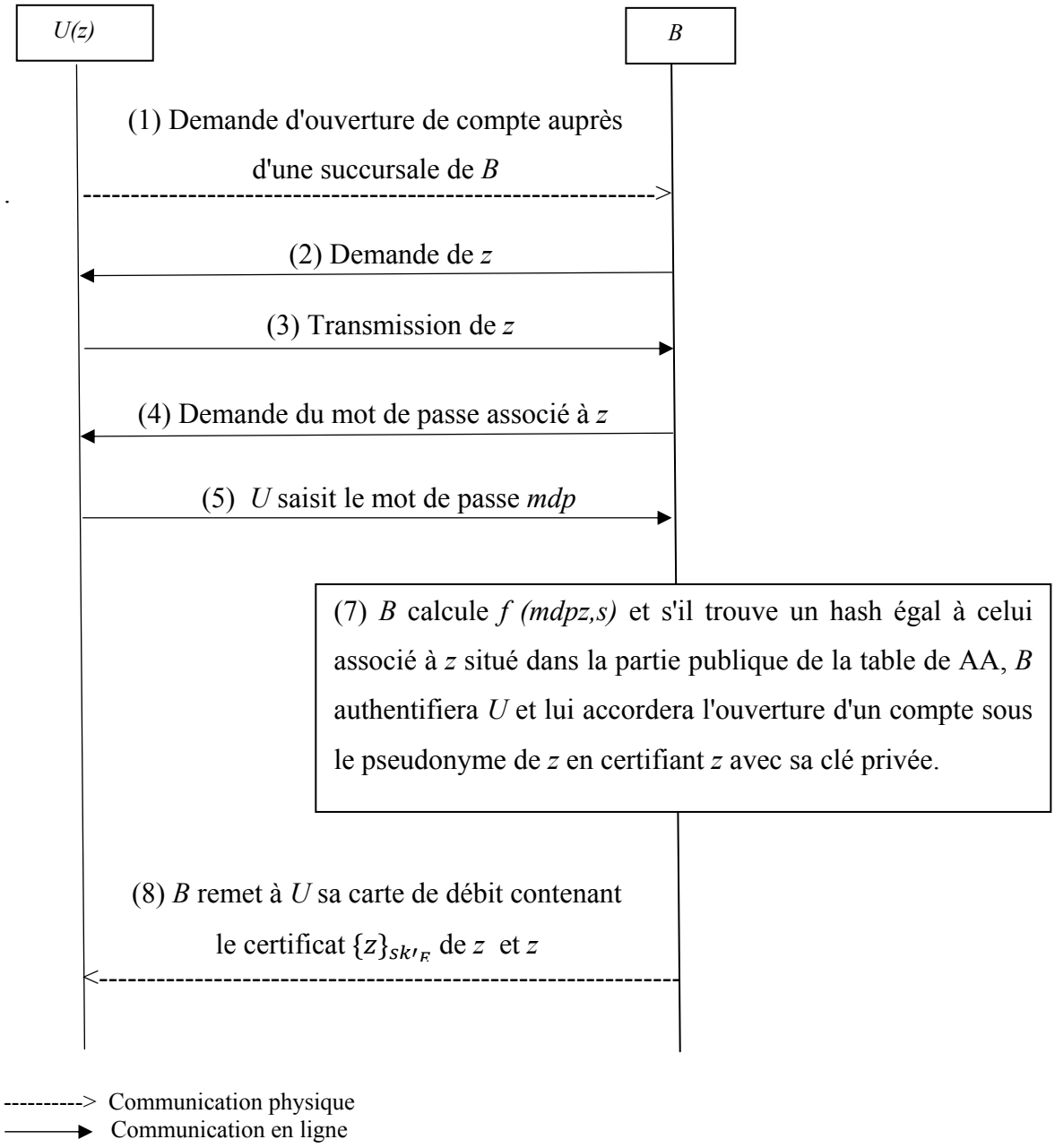

Figure 5.3. Protocole de communication entre *U* et *B*.

5.1.6. Protocole de paiement.

L'un des avantages de ce système réside dans le fait qu'il resterait pratiquement le même que celui des cartes de paiement, la différence se manifestant au niveau des données transmises. Ainsi, dans le **protocole de paiement** proposé, les données personnelles permettant d'identifier le détenteur de la carte contenues dans le couple (*données,* $\{données\}_{sk'_E}$) du protocole DDA seraient remplacées par un pseudonyme. La nécessité de mettre en place une procédure de levé d'anonymat s'impose donc et provient du fait que le pseudonyme ne contient aucune information pouvant servir à identifier l'utilisateur de la carte.

En effet, l'utilisation d'autorités de certification outre le fait de garantir l'anonymat, permettrait d'en assurer la levée en cas de fraude avérée. Celle-ci ne pourrait avoir lieu que sur demande d'une autorité gouvernementale (fisc, police, .justice..) et ce sous ordre d'un juge. Ce protocole de **révocation d'anonymat** après la phase juridique, serait l'exact opposé du protocole de création des comptes bancaires anonymes et se déroulerait principalement comme suit:

1- En cas de suspicion autour d'un compte, l'État preuves à l'appui, ferait une demande de levée d'anonymat auprès d'un juge ;
2- Si le juge estimait les preuves recevables, il délivrait alors un mandat à l'État qui s'en servirait pour demander à la banque de fournir l'identité cachée derrière le pseudonyme suspect ;
3- La banque après s'être assurée de l'authenticité du mandat, le transmettrait à l'*AA*, seule autorité de certification connaissant *w* et *z* ;
4- L'*AA* le vérifierait à son tour et déterminerait le *w* lié à *z* avant d'envoyer la demande et le *w* dont il est question à l'*AVAB* ;
5- Avant de déterminer l'identité civile associée au compte suspicieux et de fournir l'information à l'État, l'*AVAB* procèderait à un ultime contrôle du mandat.

Ce processus de levée d'anonymat rend le système proposé plus sûr et permet d'envisager sa réalisabilité d'un point de vue juridique. Hormis cela, certaines procédures de dépôt seraient problématiques. En effet, des révélations d'identité de façon non-intentionnelle pourraient se produire lors des dépôts de chèques, des dépôts directs ou encore de virements provenant des comptes traditionnels.

Pour contrer ces possibilités les deux solutions envisageables sont :

1- Soit transformer le chèque reçu en argent comptant et ce soit en le déposant dans un compte bancaire régulier avant d'effectuer un retrait en argent liquide qui sera par la suite placé sur un compte bancaire anonyme. Cette solution, pourrait aussi s'appliquer aux dépôts directs et aux virements provenant des comptes traditionnels.
2- Ou qu'il soit juridiquement permis que les pseudonymes soient marqués sur les chèques en lieu et place de toutes les informations pouvant révéler l'identité du détenteur d'un compte.

5.1.7. Analyse de la première approche.

Étant soumis aux mêmes normes de sécurité que les cartes de débit, notre système de paiement serait enclin aux mêmes menaces malgré le fait qu'il garantirait une assez forte sécurité. En dehors d'elles, il existe un risque de levée d'anonymat par la connivence des différentes parties impliquées. Pour essayer de le minimiser, l'utilisation de deux types d'autorités de certification (en plus de la banque) ne détenant chacune que des bribes d'informations sur le compte et son détenteur permettrait d'aider à acquérir la **confiance des utilisateurs**. De plus, tout comme les institutions financières traditionnelles, la banque proposant les comptes bancaires anonymes, ainsi que les autorités de certification qui lui sont associées seraient, en cas de mise en place de ce système, soumises aux lois nationales dans le cadre la protection de la vie privée [1.13]. En effet, ni la banque ni les autorités de certification ne seront en droit de collecter ou de divulguer des informations sur leurs clients sans l'aval de ces derniers ou une injonction juridique. Cette proposition protègerait de fait la **vie privée** de ses possibles futurs utilisateurs. Il serait cependant possible pour la banque de savoir qui effectue les achats, ce qui en ferait donc un système **pseudo-anonyme**. Pour exemple, si 'jeanny' achète à deux endroits différents, la banque s'en apercevrait. Néanmoins, en cas de fraude il demeure nécessaire qu'il puisse permettre de retracer l'identité. Les institutions financières ainsi que les gouvernements doivent pouvoir accéder à de tels mécanismes pour se protéger. Outre cela, en ne modifiant pas le fonctionnement des cartes de débit lors des transactions ce système obéit aux mêmes propriétés **ACID** et à la même **divisibilité** que celles-ci (voir analyse au 4.5.3).

Finalement, nous pouvons affirmer que notre proposition a pour principal avantage les bienfaits des cartes de débit, mais également le pseudo-anonymat qu'elle procure. En revanche, elle comporte aussi des inconvénients qui peuvent se classifier en deux catégories. L'inconvénient d'ordre technique le plus important est celui du transfert lié aux chèques et aux dépôts directs. À cela peuvent s'ajouter les demandes constantes de levée d'anonymat aux banques ne fixant pas de plafonds pour les montants pouvant être placés dans les comptes bancaires. Ensuite sur le plan juridique, l'article 448.1 de la loi sur les banques pourrait engendrer un blocage. En effet, elle aurait besoin d'être modifiée pour autoriser la vérification par un tiers, les banques ne conservant pas les informations sur le client qui sont plutôt détenues par un tiers de confiance.

5.2. Deuxième approche: Cartes à jetons.

La seconde approche que nous proposons consiste en la mise en place d'un système de paiement par jetons inspiré entre autres du système de carte opus (carte de transport) de la STM[13]. Tout comme la première, sa structure sera bâtie graduellement autour de ses éléments constitutifs, en allant du moyen de distribution de ces cartes au mode de communication entre la machine distributrice de jetons et les banques, avant d'aboutir aux divers protocoles du système proposé et conclure par une analyse.

Il faut toutefois noter que ces cartes à jetons seront soumises aux mêmes normes de sécurités que les cartes de paiement à puce. De plus, elles utiliseront les mêmes protocoles de communication et d'authentification que ces dernières.

5.2.1. Conception et mise en circulation.

La conception et la mise en service des cartes à jetons (JetCard) et des terminaux de recharge pourraient être assurées par n'importe quel type de société ayant une licence gouvernementale le lui permettant. Dans l'idéal, ce type de système demanderait qu'une société, autre que les banques et les services publics, en ait le monopole.

Cette société, distribuerait ainsi les cartes dans des points de vente disséminés un peu partout, pouvant même s'accorder avec les dépanneurs et autres commerces de proximité.

[13] http://www.stm.info/fr

Des terminaux de recharge dans les points névralgiques d'une ville pourraient être installés.

5.2.2. Composition du jeton.

De prime abord, il faudrait signifier que les jetons correspondraient à une unité de monnaie nationale. Ainsi par exemple, une recharge de vingt dollars canadiens (20 CAD) serait équivalente à vingt dollars canadiens (20 CAD) en jetons. Par ailleurs, le support serait une carte à puce contenant: le numéro de la carte, la clé privée de l'organisme émetteur pour des soucis d'authentification et la période de validité de la carte. De ce fait, le jeton serait une signature numérique de l'organisme d'émission sur le numéro de la carte associé à un numéro de série aléatoire attribué au jeton.

5.2.3. Description du terminal de recharge.

Le terminal de recharge serait assez simplement composé :

- d'une **interface Utilisateur** permettant de choisir le montant de la recharge, le mode paiement, de valider, modifier ou annuler la transaction ;
- d'un **lecteur de JetCard** pour identifier et recharger la carte ;
- d'un **TPE** assurant le règlement de l'achat des jetons par carte bancaire. Ce dernier sera complètement différent du lecteur de JetCard ;
- et d'un **détecteur de monnaie** qui sera chargé de reconnaitre le montant de la monnaie introduite et ce par une analyse laser des billets de banque ainsi que des propriétés physiques et chimiques des pièces de monnaie.

5.2.4. Moyen de communication.

Soient alors les trois modes de communication suivants montrant particulièrement comment les différentes parties pourraient être complémentaires tout en demeurant indépendantes.

1- **Communications entre la JetCard et le terminal de recharge JetCard et entre la carte bancaire et le TPE.** Ces deux communications ont été regroupées car, dans chacune d'elles, les échanges s'effectuent en local entre les cartes et leurs terminaux respectifs et ce de façon indépendante.

Toutefois, il subsiste une séparation qui permet de conserver les informations secrètes des différentes cartes entre les parties prenant part à l'opération. La banque n'a ainsi aucune connaissance du numéro de la JetCard. De même, la société émettrice de JetCard ne sait rien de la carte bancaire utilisée pour effectuer le paiement. Ces deux organismes ne pourraient donc pas lier carte et un jeton pour pouvoir les retracer.

2- **Communications entre les TPE et les banques.** Les communications online entre la banque et le terminal qui en sollicite l'autorisation, n'ont lieu que pour les opérations par carte bancaire excédant un certain montant, les autres se faisant offline [5.2]. Elles sont protégées par les systèmes intranet mis en place par les banques utilisant des protocoles de sécurisation de données tels que les systèmes SSL ou TLS. Par conséquent, la fuite d'informations lors de la communication entre le TPE et la banque vers le terminal JetCard est rendue impossible [5.2, 5.3].

3- **Communication entre le TPE et le terminal de recharge JetCard**. La communication entre les deux lecteurs servira à valider ou non la transaction. Celle-ci s'effectuera de façon binaire avec le 0 marquant le refus et le 1 l'acceptation. La communication est initiée par le terminal JetCard et les autorisations sont gérées par le TPE.

5.2.5. Protocole d'activation.

Après l'achat de la JetCard à un point de vente agréé, la carte se doit d'être activée avant d'être fonctionnelle. Il faut signaler que chaque carte émise disposera des mêmes informations que les cartes de paiement à puce, excepté le fait que le couple (*données,*$\{données\}_{sk'_E}$ sera constitué du numéro de la carte et de la signature de l'organisme émetteur. Il deviendra alors (*numcarte,*$\{numcarte\}_{sk'_E}$).

La carte à présent opérationnelle, devra être authentifiée et le procédé pour se faire se déroulera de la même manière que le processus DDA.

5.2.6. Protocole de recharge.

Lors de la phase de recharge, deux choix de paiement se poseront pour acquérir les jetons. Soit donc en argent comptant ou alors par carte bancaire. Ici, il sera présenté le protocole de recharge par carte de débit ou de crédit qui mettra en relation les précédentes procédures de communications :

1- Tout d'abord, l'utilisateur insérera sa carte dans le terminal de recharge ;
2- Le terminal authentifiera alors la JetCard avant de demander à l'usager le montant voulu de la recharge;
3- Celui-ci entrera par la suite le montant avant de le valider ;
4- La JetCard sera donc rechargée et conservera une copie des jetons rechargés dans une base de données provisoire contenant les jetons inactivés ;
5- Ensuite, le terminal invitera le client à choisir le moyen de paiement souhaité ;
6- Le client choisira alors de payer soit par carte débit soit par carte de crédit ;
7- D'où, le terminal de recharge de JetCard transmettra le montant au TPE pour autorisation ;
8- Celui-ci demandera à l'usager d'insérer la carte bancaire choisie, de confirmer le montant de la transaction puis de s'authentifier à l'aide de son NIP ;
9- Après validation de la transaction, le TPE demandera à l'usager de retirer sa carte et transmettra son accord au terminal de recharge;
10- Après avoir reçu du TPE la confirmation de paiement, le terminal de recharge retirera les jetons de la base de données contenant les jetons inactivés pour les mettre dans la base de données contenant les jetons activés pouvant être utilisés.

Lors de ce protocole, la JetCard est d'abord rechargée avant d'effectuer le paiement pour éviter qu'il n'y ait possibilité de relier les cartes bancaires aux jetons.

5.2.7. Protocole d'achat.

Le protocole d'achat sera presque identique à celui utilisé lors des achats effectués par les autres moyens de paiement et suivra le processus général présenté. Cependant, il faut noter que le vendeur devra posséder un compte en unité monétaire au niveau de la société émettrice de jetons. Ceci étant dit, le protocole d'achat se déroulera comme suit :

1- Le vendeur et le client commencent par s'accorder sur le montant de la transaction;
2- Deuxièmement, le vendeur entre ledit montant dans le lecteur de JetCard qui lui aura été fourni par la société émettrice ;
3- Le client n'aura donc qu'à insérer ou à passer sa carte dans le lecteur de JetCard;
4- Enfin, le lecteur débite la JetCard du client du montant inscrit par le vendeur pour en créditer le compte.

5.2.8. Analyse de la deuxième approche.

En ce qui concerne la sécurité, ce système donne certaines garanties comme le fait qu'il soit soumis aux normes sécuritaires des cartes à puce. Cependant, le manque d'authentification par NIP est l'une des failles notables, car la perte de la carte signifie aussi la perte de l'argent. Pour pallier ce problème, un procédé de désactivation pourrait être mis en place. Cela pourrait néanmoins avoir un impact sur l'anonymat. Le moyen le plus sûr serait de fixer une limite raisonnable de recharge.

Toutefois, il ne pose pas de problème en ce qui concerne la **protection de la vie privée**. En effet, s'il est mis en place, il sera non seulement soumis aux lois canadiennes en matière de protection de la vie privée [1.13] en plus de n'être pas véritablement conçu pour permettre la collecte des informations de ces utilisateurs.

De surcroît, l'essence même de ce système étant l'**anonymat**, le pseudonyme contenu dans la carte ne contient aucune donnée civile pouvant donner lieu à une quelconque identification. Eu égard au fait que la banque recharge la carte mais ignore le lieu de son utilisation et que la société émettrice quant à elle génère les jetons sans pour autant savoir à qui la carte appartient, pour qu'il y ait traçabilité, il faudrait donc qu'il existe une connivence entre la banque et la société émettrice de cartes. D'où, en comparaison de la monnaie fiduciaire, cette approche ne peut être qualifiée de parfaitement anonyme.

En revanche, les transactions effectuées grâce à ce système, respectent certaines propriétés **ACID**. En effet, elles sont atomiques car, une transaction est effectuée en totalité ou pas du tout. Par ailleurs, elles sont tout aussi cohérentes vu le montant débité sur la JetCard correspond au montant crédité au compte du vendeur. Toutefois, deux opérations ne pouvant être réalisé simultanément, elles ne sont ainsi pas isolées.

Malheureusement du point de vue du client, elles ne sont pas non plus durables, puisque ce dernier n'a accès à aucun historique de dépenses. Par contre, elles le sont du point de vue de la société émettrice qui conservera l'historique des transactions effectuées par une carte (ceci peut se révéler utile en cas de détection de fraude).

Étant donné que ce système serait rattaché à une unité monétaire nationale, sa **divisibilité** serait de fait évidente, quoiqu'il ne soit pas possible de faire des achats en centimes par exemple, il faudrait faire un arrondi à une valeur supérieure ou inférieure selon le cas.
En définitive, nous pourrons dire que ce système a des avantages au rang desquels nous citerons l'anonymat, la rapidité des transactions et le fait qu'il représenterait une alternative à la monnaie fiduciaire. Malheureusement, il n'en demeure pas moins qu'il présente tout de même des inconvénients, principalement l'impossibilité de transformer des jetons en monnaie traditionnelle ou encore la perte d'argent entrainée par l'égarement de la JetCard.

5.3. Système hybride.

Lors de la présentation des deux premières approches, nous avons rencontré le problème du transfert relativement aux comptes bancaires anonymes et celui de la conversion des jetons en argent comptant dans l'approche des cartes à jetons. Pour les résoudre, un mécanisme de juxtaposition a été pensé.
Ainsi, la machine idéale serait celle qui contiendrait les trois axes suivant fonctionnant concomitamment et qui serait indépendamment gérer par les différents organismes.
Soit alors :

1- La réception d'un virement bancaire ou le dépôt d'un chèque qui se ferait dans un compte bancaire normal. Après crédit de son compte, le détenteur d'une JetCard (Jet-compte) émettrait l'ordre à sa banque d'effectuer l'achat de jetons pour le montant désiré ;

2- La compagnie émettrice de jetons enverrait alors l'autorisation de fabriquer des jetons, au Jet-compte associé. Pour des raisons de clarté, mentionnons que la société émettrice de jetons n'a uniquement connaissance que de l'identité de la banque de laquelle provient l'ordre, quant à la banque du demandeur elle émet l'ordre sans en connaitre le pseudonyme associé à la carte inclus dans le jeton ;

3- La troisième et dernière phase consistera au déplacement des jetons vers un compte bancaire anonyme à transfert c'est-à-dire capable d'effectuer une transformation du jeton en toutes ses autres formes possibles.

L'avantage d'un tel système, outre le fait qu'il permettrait de réintroduire des jetons dans un système bancaire plus conventionnel si besoin est, octroierait par la même occasion une possibilité de transfert vers des comptes bancaires anonymes, sans pour autant révéler l'identité du propriétaire ou être la porte d'entrée d'une intrusion dans sa vie privée. Le véritable plus que ce système apporterait est qu'il bénéficierait de la sécurité imposée aux trois sous-systèmes le composant.
Il n'est cependant pas parfait et regorge d'inconvénients dont le plus sérieux reste la lourdeur associée à chaque opération à une époque où la rapidité est de mise ; Ce qui serait indubitablement un frein. À cela, associez les coûts liés au déploiement de telles machines et vous comprendrez que sa réalisation ne sera point aisée.

Dans le courant de ce chapitre, nous avons émis des hypothèses pour essayer de solutionner les problèmes auxquels font face les moyens de paiements, et ce en proposant deux approches distinctes. Un troisième système hybride et à cheval sur ces prédécesseurs s'est vu également émettre. Malheureusement, ce dernier lui-aussi fut mis en difficulté.
Face à une telle situation, on est alors amener à se demander si la résolution des problèmes du de l'hybride pourrait déboucher sur un système de paiement consensuel et adopté de tous ?

Conclusion

L'objectif de ce mémoire était une analyse comparative des principaux moyens de paiement dont nous disposons aujourd'hui afin d'en déterminer les forces et les faiblesses. De ce travail, sont ressorties les réponses aux questions posées en introduction grâce à des aspects tels que l'anonymat, la confiance des utilisateurs (sécurité), la protection de la vie privée ou encore le respect des propriétés ACID.

Dès lors, à la question de savoir quel est le moyen de paiement garantissant un anonymat total nous sommes en mesure de répondre qu'il s'agit de la monnaie fiduciaire. Effectivement, elle apparaît comme étant le seul moyen de paiement qui ne relie en aucun cas l'utilisateur à l'achat effectué; En un mot, elle est non-traçable.

En portant notre attention sur la protection de la vie privée, nous remarquons que la monnaie fiduciaire se place encore une fois dans le haut du tableau, même si celle-ci n'est pour ainsi dire pas réellement concernée par ce critère, puisqu'elle ne collecte ni ne conserve d'informations de ses utilisateurs, à contrario des monnaies dites électroniques. Excepté bitcoin, dont le principe repose sur la publication de transactions effectuées, les organismes émetteurs de tous les autres moyens de paiement sont soumis aux lois sur la collecte et la protection des informations. De fait, il est le seul à ne pas garantir la protection de la vie privée.

Concernant les propriétés ACID, nous pouvons affirmer sans doute aucun, que les cartes de débit et bitcoin sont ceux qui les respectent le mieux. C'est-à-dire qu'ils sont les seuls à obéir aux règles d'atomicité, de cohérence, d'isolation et de durabilité.

Cependant, du point de vue sécuritaire, il est difficile de se prononcer sans équivoque. En effet de nos analyses, nous retenons que ces moyens de paiement mettent en place des mesures de sécurité efficaces adaptées aux technologies qu'ils utilisent. Néanmoins, les cartes de débit et de crédit, en utilisant un système d'authentification de la carte et de son détenteur lors des transactions, offrent une garantie de sécurité en cas de perte ou de vol de la carte. Garantie que n'offrent pas les autres moyens de paiement.

Retenons en substance de notre randonnée intellectuelle que les cartes de débit et de crédit sont les plus avantageuses malgré qu'elles ne procurent pas d'anonymat, car hormis le fait qu'elles confèrent une sécurité accrue, elles peuvent en plus être utilisées à l'international et nous épargner le transport de l'argent comptant.

Au terme de ce travail analytique, deux alternatives de paiement qui modifieraient les systèmes en place furent proposées. En premier lieu, nous avons mis en avant un système d'ouverture de comptes bancaires anonymes permettant la modification des cartes de débit pour les rendre semi-anonymes. En effet, les données personnelles du client servant à son identification seront remplacées par un pseudonyme validé par une autorité de certification après vérification des informations du client. Ce pseudonyme sera communiqué à la banque qui l'utilisera pour ouvrir un compte au client.

En second lieu, nous avons développé un système avec comme principe les cartes à jetons à l'instar des cartes opus de la STM. Contrairement au premier, il sera complètement anonyme, arrimant toutefois le handicap majeur qu'est l'impossibilité de retransformer les jetons en monnaie fiduciaire. Enfin, à leur suite, nous en avons proposé un troisième qui les combinait. Ce système concédait non seulement la reconversion des jetons en argent comptant sans pour autant en compromettre l'anonymat, mais aussi de faire des dépôts de chèques dans les comptes bancaires anonymes en les ayant d'abord transformer en jetons.

En définitive, au travers de notre contribution, nous avions voulu amener du neuf à des idées déjà existantes. Certes, nombre d'améliorations restent à apporter pour que les systèmes proposés soient véritablement viables. Pour cela, il faudrait avant tout que les lois les permettent.

Bibliographie

[1] C. Dragon, D. Geiben, D. Kaplan, G. Nallard, « *Les moyens de paiements, Des espèces à la monnaie électronique* », Banque editeur, pp. 18-63, 1997.

[2] J-B. Bosquet-Denis, *« Droit pénal des affaires en Chine* », Éditions Amalthée, p.39, 2011.

[3] J-P. Toernig, F. Brion, « *Les moyens de paiement* », Presses universitaires de France éditeur, pp.11- 17, 1999.

[4] S. Piedelièvre, « *Instruments de crédit et de paiement* », Dalloz éditeur, 5ème édition, pp. 253-264, 2007.

[5] P. Bresse, G. Beaure d'Augères, S. Thuillier, « *Paiement numérique sur internet* », International Thomson Publishing , 299 pages, 1997.

[6] S. Miranda, « *Base de données, architectures, modèles relationnels et objets, SQL 3* », Dunod éditeur , pp. 286-292, 2002.

[7] S. Calé, P. Touitou, « *La sécurité informatique: réponses techniques, organisationnelles et juridiques* », Hermés science publication , pp. 87-98, 2007.

[8] Union Internationale Des Télécommunications, « *X.800 : Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT* », UTI éditeur, pp. 6-35, 1991.

[9] L. Law, S. Sabett, J. Solinas, « *How to make a mint: The cryptography of anonymous electronic cash* », National Security Agency éditeur, pp. 4-33, 1996.

[10] G. W. Hansen, J. V. Hansen, « *Database Management and Design* », Prentice Hall Editions, 2ème édition, pp. 137-145, 1996.

[11] G. Riccardi, « *Principales of Database Systems with internet and java Application s*», Addison Wesley Publishing Company éditeur, pp. 355-379, 2001.

[12] J. Gray, « *The Transaction Concept: Virtues and Limitations* », dans proceedings of the seventh international conference on Very Large Data Bases, volume 7, pp. 144-154, 1981.

[13] Association des Banquiers Canadiens, « *Le système de paiements efficace du Canada* », Association des Banquiers Canadiens, pp. 1-4, 2014.

[14] Union des consommateurs, « *Nouveaux modes de paiements : le Canada est-il prêt?*», Union des consommateurs, pp. 19- 47, 2011.

[15] G. Gobin, « *Les opérations bancaires et leurs fondements économiques* » dunod éditeur, pp.9-292, 1980.

[16] Banque du Canada, « *Levons le voile sur les nouveaux billets canadiens en polyméres* », Banque du Canada, pp. 1-2, 2011.

[17] Gendarmerie Royale Du Canada, « *Nouveaux billets de banque anti-contrefaçon*», La Gazette,volume 74, no. 3, p.36, 2012.

[18] G. Quaden, « Coûts*, avantages et inconvenients des differents moyens de paiement*», Banque Nationale de Belgique, pp. 23-60, 2005.

[19] D. Pointcheval, « *Les preuves de connaissances et leurs preuves de sécurité: thèse de doctorat* », Université de Caen, pp. 12-36, 1996.

[20] T. Brunet, Y. Metay, F. Moine , « *Économie Droit* », Bréal éditeur, p. 137, 2006.

[21] J.-L.Bailly, G. Caire, A. Figliuzzi, V. Lelièvre, « *Économie monétaire et financière* » Bréal éditeur, pp. 50-160, 2006.

[22] J. Stoufflet, Christian Gavalda, «*Instrument de paiement et de credit* », LexisNexiz éditeur, 7ème édition, pp. 1-12, 2009.

[23] G. Lengendre, « *Instruments de paiement et de crédit : le chèque, la lettre de cahnge, le billet à ordre* », Dumond éditeur, pp. 15-129, 1969.

[24] CCI D'Alsace, « *Chèque condition de validité quant à sa forme* » dans les notes d'information juridiques du 28 septembre 2014, CCi Alsace, pp. 2-10, 2014.

[25] Association Canadienne des Paiements, « *Norme 006 Spécification pour les documents codé à l'ancre* », Association Canadienne des Paiements, pp. 5-130, 2013.

[26] Gouvernement du Québec, *« Loi sur la protection des renseignements personnels dans le secteur privée* » © Éditeur officiel du Québec, Quèbec, 2014

[27] M.-A. d. Cockborne, « *Tout sur le chèque et ses infractions* », De Vecchi SA éditeur, pp.3-199, 1973.

[28] M. Cabrillac, *« Le chéque et le virement* » Litec éditeur, 5ème édition, pp. 10-199, 1980.

[29] P. Barthélémy, R. Rolland, P. Véron, « *Cryptographie principes et mises en oeuvre*», Lavoisier éditeur, pp. 23-169, 2005.

[30] G. Dubertret, «*Initiation à la cryptographie* », Vuibert éditeur, 3ème édition pp. 23-115, 2002.

[31] S. Heraud, « *Vérification semi-automatique de primitives cryptographiques: thèse de doctorat*», Université Nice Sophia Antipolis, pp. 31-55, 2012.

[32] Aiden A. Bruen, Mario A. Forcinito « *Cryptography, information theory and error correction* », wiley & Sons editions, pp. 56-368, 2005.

[33] Y. L. Jonatahn Katz, « *Introduction To Modern Cryptography* » Charpman & Hall/CRC éditeur, pp. 240-290, 2008.

[34] G. Dhillon, « *Principles of Information Systems Security text and Cases* », wiley & Sons editions , pp. 46-60, 2007.

[35] D. Stinson, « *Cryptographie théorie et pratique* », vuibert éditeur, pp. 16 -337, 2003.

[36] M. Atreya, B. Hammond, S. Paine, P. Starrett, S. Wu, « *Digital signatures* », RSA press éditeur, pp. 23-82, 2002.

[37] R. J. Spillman, « *Classical and contemporary cryptology* », Pearson Prentice Hall éditeur, pp. 221-254, 2005.

[38] American Mathematical Society, « *Applied cryptology, cryptographic protocols, and computer security models* », American Mathematical Society éditeur, volume 29 , pp. 8-179, 1983.

[39] B. A. Forouzan, « *Cryptography and Network Security* », Mc Graw Hill éditeur, pp. 301-314, 2008.

[40] D. O'Mahony, M. Peirce, H. Tewari, « *Electronic Payments Systems for E-Commerce* », Atech house éditeur, Second edition, pp. 34-47, 2001.

[41] P. Wayner, « *Digital Cash* », Byte éditeur, Vol.19, p.126., 1994.

[42] B. Schoenmakers, « *Basic Security of the ecash Payment System, Computer security and industrial Cryptography: State of the art and evolution* », dans LNCS series 1997 , pp. 338-356, 2014.

[43] A. F. M. N. David Chaum, « *Untraceable Electronic Cash, Advances in CRYPTO '88* » dans LNCS Spinger-Verlag, pp. 319-327, 1988.

[44] M. H. Shérif, « *Paiements électroniques sécurisés* », Presses polytechniques et universitaires romandes éditeur, pp. 44-142, 2007.

[45] L. Jean Camp, M.Sirbu, J.D. Tygar, «*Token and Notational Money in Electronic Commerce*» dans Proceedings of the First USENIX Workshop in Electronc Commerce, pp. 1-12, 1995.

[46] D. Chaum, « *Achieving Electronic Privacy* », dans Scientific American August 1992, pp. 96-101, 1992.

[47] M. J. Farsi, « *Digital Cash Master's Thesis in Computer Science* », Goteborg University, pp. 8-48, 1997.

[48] K. Schemeh, « *Cryptography and public key infrastructure on the internet* », Wiley & Sons éditeur, pp. 433-437, 2001.

[49] Wang, S. Lo, J.Christina, « *Bitcoin as Money* », dans Federal Reserve Bank of Boston, No. 14-4, pp. 8-28, 2014.

[50] D. Descouteaux, « *Bitcoin: plus qu'une monnaie, un potentiel d'innovation* » dans les notes économiques de janvier 2014, Institut Economique de Montreal, 2014.

[51] E.Androulaki, Ghassam O. Karame, M. Roeschlin, T. Scherer, S. Capkun,

« *Evaluating User Privacy in Bitcoin* » dans Financial Cryptography and Data Security, Volume 7859 de la série Lecture Note in Computer Science, pp. 34-51, 2013.

[52] J. P. Delahaye, « *Le Bitcoin, une monnaie révolutionnaire?* », dans UMR 8022 CNRS, Laboratoire d'informatique fondamentale de Lille, pp. 11-51, 2014.

[53] M. H. Fergal Reid, « *An Analysis of Anonymity in the Bitcoin System* », dans

IEEE Computer Society, International Conference on Privacy Security Risk and Trust and IEEE International Conference on Social Computing , pp. 1318-1326, 2011.

[54] T. Patron, « *The Bitcoin Revolution: An internet of money* », Kindley Edition, pp. 12-130, 2014.

[55] Banque de France Eurosystème, « *Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin* » dans Focus Numéro 10, pp. 1-6, 2013.

[56] W. Kim, H. Kim, « *Smart Cards : Status, Issues, and US Adoption* », dans Journal of Object Technologie, volume 3, Numéro 5, pp. 25-30, 2004.

[57] Z. Chen, « *Java Card Technology for smart Cards, Architecture and Programmer's Guide* », Sun éditeur, pp 3-26 , 2000.

[58] C. Tavernier, «*Les cartes à puce*», Dunod éditeur, 2é édition, pp. 14-68, 2007.

[59] J. Ferrari, R. Mackinnon, S. Poh, L.Yatawara, « *Smart Cards: A Case Study* », International Technical Support Organization éditeur, first édition, p.7, 1998.

[60] C. Tavernier, « *Les cartes à puce, guide du concepteur et du developpeur* », Dunod éditeur, pp. 68-89, 2002.

[61] X. Kauffmann-Tourkestansky, « *Analyses sécuritaire de code de carte à puce sous attaques physiques simulées : Thése de Doctora*t », Université d'Orléans, pp. 15-69, 2012.

[62] W. Rankl, W. Effing, « *Smart Card Handbock* », Wiley & Sons éditeur, pp. 153-489,1997.

[63] C. Anastasia, C. Nikolaos, G. Theodora, « *The use of smart cards and their implications on the society* », NETIS éditeur, pp. 2-30, 2008.

[64] Direction Centrale de la sécurité des systèmes d'informations, « *Prise en compte des correctifs du logiciel Embarqué, Chargés en EEPROM, lors de l'évaluation d'une carte à puce selon le PP9911*»,Sécrétariat général à la défense nationale République Française éditeur, pp. 1-6, 2006.

[65] Smart Card Alliance, «*Card Payments Roadmap in United States: How will EMV impact the future payments infrastructure?* », Smart Card Alliance éditeur, pp. 8-35, 2006.

[66] S. J. Murdoch, S. Drimer, R. Anderson, M. Bond, « *Chip and PIN is broken* », dans IEEE Computer Society, IEEE Symposium on Security and Privacy, pp. 433- 446, 2010.

[67] K. Mayes, K. Markantonakis, « *Smart cards, Tokens, Security and Applications* », Spingers éditeur, pp. 20-370, 2008.

[68] M. S. Bhuiyan, «*Securing Mobile payment Protocol based on EMV Standard: Master thesis* » Royal Institute of technology, pp. 15-36, 2012.

[69] Pool, J. de Ruiter and Erick, «*Formal Analysis of the EMV protocol Suite. In theory of security and Applications*», dans TOSCA, LNCS volume 6993, pp. 113-129, 2012.

[70] R. Morris, K. Thomson, « *Password Security : A Case History* »,

dans Communications of the ACM du 22 Novembre 1979 , pp. 594- 597, 1979.

Documents internet

[1.1] Larousse, « *Dictionnaire Français* », consulté le 02 décembre 2014. [En ligne]. http://www.larousse.fr/dictionnaires/francais.

[1.2] Banque du Canada, « *Glossaire* », consulté le 02 Décembre 2014. [En ligne]. http://www.banqueducanada.ca/publication/glossaires/glossaire/.

[1.3] Fédération Bancaire Française, « *Lexique* », consulté le 02 Décembre 2014. [En ligne]. http://www.fbf.fr/fr/accueil.

[1.4] BeCompta, « Compte bancaire », consulté le 15 Décembre 2014. [En ligne]. http://www.becompta.be/dictionnaire/compte-bancaire.

[1.5] M. Ryan, « *Digital Cash* »,consulté le 02 Décembre 2014. [En ligne] http://www.cs.bham.ac.uk/~mdr/teaching/modules06/netsec/lectures/DigitalCash.html.

[1.6] Ministère de la justice du Canada, « *Loi sur la Banque du Canada* », consulté le 25 Novembre 2014. [En ligne]. http://laws-lois.justice.gc.ca/PDF/B-2.pdf.

[1.7] Monnaie Royale Du Canada, « *Production de pièces* », consulté le 10 Décembre 2014.

[En ligne]. http://www.mint.ca/store/mint/learn/production-de-pieces-1200012?lang=fr_CA#.VIYgOjHF-y4.

[1.8] Gouvernement du Canada, « *Plan d'action économique du Canada* », consulté le 08 Décembre 2014. [En ligne].http://actionplan.gc.ca/fr.

[1.9] Ministère de la justice du Canada, « *Site Web de la legislation (Justice)* », consulté le 08 Décembre 2014. [En ligne]. http://laws-lois.justice.gc.ca/fra/lois/c-46/page-208.html.

[1.10] Association des Banquiers Canadiens, « *Évitez les faux billets* », consulté le 09 Décembre 2014. [En ligne].

http://www.cba.ca/fr/consumer-information/42-safeguarding-%20your-money/92-avoiding-counterfeit-bills.

[1.11] Desjardins, « *Exemplaire de chéque* », consulté le 07 Mai 2014.[En ligne]. http://images.desjardins.com/fr/pict/1d03_cheque2009.gif.

[1.12] Associantion des Banquiers Canadiens, « *Tout ce que vous voulez savoir à propos des chèques* », consulté le 28 Décembre 2014. [En ligne].http://www.cba.ca/fr/consumer-information/40-banking-%20basics/584-cheques-what-you-need-to-know.

[1.13] Commissariat à la protection de la vie privée du Canada, « *Lois sur la protection des renseignements personnels au Canada* » consulté le 15 Mai 2014.[En ligne]. https://www.priv.gc.ca/cf-dc/2001/cf-dc_010814_02_f.asp.

[2.1] secureinfo.com, « *Introduction et initiation à la sécurité informatique*», consulté le 30 Juillet 2014. [En ligne]. https://www.securiteinfo.com/conseils/introsecu.shtml.

[2.2] cryptage.org, « *L'analyse des frèquences* », consulté le 15 Juillet 2014. [En ligne]. http://www.cryptage.org/analyse-frequentielle.html.

[2.3] G. Labouret, « *Introduction à la cryptologie* », consulté le 5 Novembre 2014. [En ligne]. http://www.labouret.net/crypto/#341.

[2.4] Senat Republique Française, « *La sécurité des transactions réalisées par carte bancaire* », consulté le 5 Novembre 2014. [En ligne]. http://www.senat.fr/lc/lc125/lc125_mono.html.

[2.5] J. Stern, L. Granboulan,P. Nguyen,D. Pointcheval, « *Conception et preuves d'algorithmes* » 2004. consulté le 16 Juillet 2014 [En ligne]. http://www.di.ens.fr/~wwwgrecc/Enseignement/CoursCryptoMMFAI.pdf.

[2.6] E. Bresson, «*cryptographie chiffrement symetrique* », consulté le 10 Janvier 2014 [En ligne]. http://www.di.ens.fr/~bresson/P12-M1/P12-M1-Crypto_3.pdf.

[2.7] Gouvernement de la République Française, « *Fonction de Hachage* », consulté le 05 Décembre 2014. [En ligne]. http://www.securite-informatique.gouv.fr/autoformations/cryptologie/co/cryptologie_CH03_SCH02_U02.html.

[2.8] Association de Cryptographie Théorique et Appliquée, « *Lexique* », consulté le 20 Juillet 2014. [En ligne]. http://www.acrypta.com/index.php/lexique.

[2.9] M. C. John Black, « *MAC Reforgeability* », International Association for Cryptologic Research Publication, consulté le 30 Juillet 2014. [En ligne]. https://eprint.iacr.org/2006/095.pdf.

[2.10] D. Chaum, «*Security without Identification Card Computer to Make Big Brother Obselete*», consulté le 06 Décembre 2014. [En ligne]. http://www.chaum.com/articles/Security_Wthout_Identification.htm.

[3.1] D. Chaum, « *profile* » consulté le 12 Décembre 2014. [En ligne]. http://www.chaum.com/#profile.

[3.2] D. Chaum, « *Online Cash Checks* », consulté le 10 Décembre 2014. [En ligne]. http://www.chaum.com/articles/Online_Cash_Checks.htm.

[3.3] Bitcoin.org, « *Foire aux Questions* », consulté le 10 Décembre 2014. [En ligne]. https://bitcoin.org/fr/faq#qui-controle-le-reseau-bitcoin.

[3.4] F. Stlder, « *Digicash: Failure is interesting* », consulté le 10 Décembre 2014. [En ligne]. http://felix.openflows.com/html/digicash.html.

[3.5] M. Rosenfeld, « *Overview of Colored Coins* », consulté le 10 mai 2014 [En ligne]. https://bitcoil.co.il/BitcoinX.pdf, December 4, 2012.

[3.6] S. Nakamoto, « *Bitcoin: A peer-to-peer Electronic Cash System* », consulté le 10 mai 2014 [En ligne]. https://bitcoin.org/bitcoin.pdf.

[3.7] Shamir, D. Ron, Adi « *Quantitative Analysis of the Full Bitcoin Transaction Graph* », consulté le 10 mai 2014 [En ligne]. https://eprint.iacr.org/2012/584.pdf.

[3.8] Bitcoin, « *Comment fonctionne bitcoin* », consulté le 13 Décembre 2014. [En ligne]. https://bitcoin.org/fr/faq#comment-fonctionne-bitcoin.

[3.9] M. Nielsen, «*How the Bitcoin protocol actually works*», consulté le 12 Décembre 2014. [En ligne] . http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/.

[3.10] Toutsurlebitcoin.com, « *La chaine de blocs* », consulté le 13 Décembre 2014. [En ligne].http://www.toutsurlebitcoin.com/la-chaine-de-blocs-blockchain.

[3.11] bitcoin.fr, « Principes et techniques » consulté 13 Décembre 2014. [En ligne]. http://www.bitcoin.fr/pages/Principes-techniques.

[3.12] S. Nakamoto, « Bitcoin expliquer par son inventeur », consulté le 10 Décembre 2014. [En ligne]. http://www.bitcoin.fr/pages/Bitcoin-expliqu%C3%A9-par-son-inventeur.

[3.13] Y. Guerrini, « Bitcoin, Litecoin : la folie des cryptomonnaies » consulté le 13 Décembre 2014. [En ligne] http://www.tomshardware.fr/articles/bitcoin-miner-litecoin,2-892-3.html.

[3.14] bitcoin, «*Protéger votre confidentialité*», consulté le 13 Décembre 2014. [En ligne]. https://bitcoin.org/fr/proteger-votre-vie-privee.

[3.15] I. Burgun, « *Les jours noirs de la crypto-monnaie* », consulté en le 15 Novembre 2014. [en ligne]. http://www.sackvilletribunepost.com/Opinion/Chroniques/2014-03-07/article-3641203/Les-jours-noirs-de-la-crypto-monnaie/1.

[3.16] A. Fournier,« *Comment la France veut réguler le bitcoin* », consulté le 20 Décembre 2014 [en ligne] http://www.lemonde.fr/economie/article/2014/07/11/comment-la-france-veut-reguler-le-bitcoin_4455225_3234.html.

[3.17] Journal lesechos.fr, « *Chine: Alibaba interdit le paiement en Bitcoins* », consulté le14 Décembre 2014. [En ligne]. http://www.lesechos.fr/08/01/2014/lesechos.fr/0203229211414_chine---alibaba-interdit-le-paiement-en-bitcoins.htm.

[4.1] T. Martin, «*Le b.a ba de la RFID Origines, Technologies et Applications*», consulté le 13 Décembre 2014. [en ligne]. http://blogresearch.smalsrech.be/publications/document/?docid=87.

[4.2] IBM, « *ANSI X9.17 Key Management Services* », Consulté le 12 Décembre 2014. [En ligne]. http://www-01.ibm.com/support/knowledgecenter/SSLTBW_2.1.0/com.ibm.zos.v2r1.csfb400/axkms.htm%23axkms.

[4.3] Visas Canada, «*La norme EMV*», Consulté le 16 Décembre 2014. [En ligne].http://www.visa.ca/puce/titulaires-de-carte/la-norme-emv/index.jsp.

[4.4] EMVco,« *EMV Integrated Circuit Card Spécifications for Payments Systems Book 2 Security and Key Management version 4.2* »,consulté le 16 Janvier 2015. [en ligne]. http://www.emvco.com/specifications.aspx?id=155.

[4.5] EVMco, « *EMV 2008 Integrated Circuit Card Speécification Card for Payment System, Book 3 - Application Spécification, version 4.2* »,consulté le 8 mars 2015 [en ligne]. http://www.emvco.com/specifications.aspx?id=155, 2008.

[4.6] C. M. Khuong An Nguyen, « *EMV (Chip and PIN) Project* », consulté le 17 Décembre 2014. [En ligne]. http://www.academia.edu/373702/EMV_Chip_and_PIN_survey.

[4.7] Banque Nationale du Canada (BNC), « *Carte à puce* », consulté le 26 Mai 2014. [En ligne].http://www.bnc.ca/content/public/fr/particuliers/cartes-de-credit/cartes-de-credit mastercard/guides-et-outils/carte-a-puce.html.

[4.8] Interact , « *Débit Interac pour les consommateurs* », consulté le 17 Décembre 2014. [En ligne]. http://www.interac.ca/index.php/fr/debit-interac/debit-interac-pour-les-consommateurs#Pourquoi-utiliser-Debit-Interac.

[4.9] Interac, « *Sécurité* », consulté le 17 Décembre 2014. [En ligne]. http://www.interac.ca/fr/securite.

[4.10] Association des Banquiers Canadiens, « *La fraude par carte de débit* », consulté le 17 Décembre 2014. [En ligne]. http://www.cba.ca/fr/consumer-information/42-safeguarding-your-money/59-debit-card-fraud.

[4.11] Association Coopérative d'Économie des Basses-Laurentides, *« Un compte de banque, c'est un droit! les moyens pour défendre vos droits* », consulté le 17 Décembre 2014. [En ligne]. http://www.faillitequebec.com/fichier/Compte-de-banque-Moyens-vs-droits.pdf.

[4.12] Visa, « *Cardholder FAQs* », consulté le 15 Décembre 2014. [En ligne]. : http://www.visa.ca/en/personal/securewithvisa/vbv/faqs.jsp.

[4.13] Mastercard, « *Mastercard securecode enhaned security for online shopping* », consulté le 15 Décembre 2014. [En ligne]. http://www.mastercard.ca/securecode.html.

[4.14] Allopass, «F.A.Q. marchant », consulté le 17 Décembre 2014. [En ligne]. http://www.allopass.com/fr/support/faq/merchant#q0001.

[4.15] Gendarmerie Royale du Canada, « *La fraude par carte de crédit* », consulté le 17 Décembre 2014. [En ligne].http://www.rcmp-grc.gc.ca/scams-fraudes/cc-fraud-fraude-fra.htm.

[4.16] Association des Banquiers Canadiens, « *Les cartes de crédit : statistiques et données* », consuté le 17 Décembre 2014. [En ligne]. http://www.cba.ca/fr/media-room/50-backgrounders-on-banking-issues/123-credit-cards.

[5.1] Ministère de la justice du Canada, « *Règlement sur l'accès aux services bancaires de base* », consulté le 22 Décembre 2014. [En ligne]. http://laws-lois.justice.gc.ca/fra/reglements/DORS-2003-184/page-1.html.

[5.2] The Apache Software Foundation, « Chiffrement SSL/TLS fort : Introduction », consulté le 23 Décembre 2014. [En ligne]. http://httpd.eu.apache.org/docs/trunk/fr/ssl/ssl_intro.html.

[5.3] Gouvernement Français, « *Les protocoles réseau* », consulté le 28 Décembre 2014. [En ligne]. http://www.securite-informatique.gouv.fr/autoformations/securite_reseaux/co/secu_reseaux_1_ch01_uc03.html

Annexes

Étant donné le volume des documents, nous trouvons plus adéquat que de ne référencer que les liens internet.

Annexe A : Recommandations x.800.

http://www.itu.int/rec/T-REC-X.800-199103-I/fr

Annexe B : Feuilles de travail : Contrefaçon des billets de banques émis par la banque du canada.

http://www.banqueducanada.ca/wp-content/uploads/2013/09/contrefacon-billets-banque.pdf

Annexe C : Spécifications EMV pour les cartes de paiement à puce.

http://www.emvco.com/download_agreement.aspx?id=652