Sistemes de pagament electrònic

Josep Lluís Ferrer Gomila
Llorenç Huguet Rotger
M. Magdalena Payeras Capellà

PID_00199769

UOC
Universitat Oberta de Catalunya

Índex

Introducció

Amb l'aparició i generalització del comerç electrònic s'ha fet necessària la creació de sistemes electrònics de pagament adaptats a la situació no presencial dels usuaris involucrats. Amb els pagaments electrònics es pretén aconseguir un mitjà de pagament que presenti un conjunt de característiques propi dels sistemes de pagament físics, alhora que permeti realitzar transaccions sense que els usuaris es trobin físicament, és a dir, que es permetin transaccions remotes.

Els sistemes de pagament electrònic presenten molta diversitat. Alguns d'ells es basen en la infraestructura de targetes bancàries existents, mentre que altres intenten emular les prestacions de la moneda física. En qualsevol dels casos s'haurà de garantir la seguretat del sistema. Les mesures de seguretat criptogràfiques substitueixen (o complementen) les mesures de seguretat físiques, com ara els hologrames, els fils de seguretat o les marques d'aigua en la moneda física i les bandes magnètiques i els xips en les targetes de crèdit o dèbit.

La moneda física és un mitjà de pagament tradicional, que presenta com a característica important (a diferència d'altres sistemes de pagament) la possibilitat de realització de pagaments anònims. Aquesta serà una característica desitjable a l'hora de construir un nou mitjà de pagament electrònic.

Altres mitjans de pagament habituals en el món físic podrien ser utilitzats en transaccions remotes. Les targetes bancàries en són un exemple. A diferència de la moneda física, les targetes bancàries no són anònimes i permeten el monitoratge de les transaccions i la creació de perfils de clients, a causa de la possibilitat d'enllaç dels diferents pagaments realitzats pel mateix usuari. També s'haurà de tenir en compte que les mesures de seguretat basades en la presència física de la targeta (banda magnètica, xip) no s'utilitzen en aquestes transaccions a no ser que es disposi d'un lector de targetes. La seguretat basada en la presència física es pot substituir per l'ús de tècniques de seguretat no presencials. Si no és així, la utilització de manera autònoma del número de la targeta presenta problemes d'autorització del pagament.

1. Tipus de sistemes de pagament electrònic

Entre els pagaments electrònics es poden distingir diverses categories. La classificació es pot fer en funció de diferents criteris, tenint en compte el marge de quantitats dels pagaments que es poden realitzar en el sistema, així com la semblança i la utilització d'elements de mitjans de pagament convencionals. L'eficiència i els costos associats a les transaccions realitzades amb les diferents categories condicionen la magnitud dels pagaments que es poden realitzar amb cadascuna d'elles. D'aquesta manera uns costos associats elevats impliquen un límit inferior en la magnitud dels pagaments i impossibiliten pagaments de petites quantitats. Per altra part, la reducció de mesures de seguretat permet reduir els costos i millorar l'eficiència però, com a conseqüència, no permet realitzar pagaments de grans quantitats de manera totalment segura.

Una de les tres barreres existents que limiten l'extensió del comerç electrònic, junt amb la facilitat d'ús i l'accés al maquinari requerit, és la manca de privacitat. Per aquest motiu, un altre aspecte diferenciador en els sistemes de pagament electrònic és el grau de privacitat que ofereixen. Ens trobem amb sistemes on els usuaris són totalment identificats, amb sistemes que permeten que el pagador es mantingui anònim davant del receptor del pagament, però que exigeixen que s'identifiquin enfront del banc (i com a conseqüència el banc és capaç de relacionar el pagador amb un dipòsit del receptor del pagament) o bé amb sistemes totalment anònims on no es pot descobrir la relació entre un comprador i la compra realitzada. Una altra propietat a tenir en compte és la possibilitat d'ús anònim dels diners rebuts en un pagament.

La presència o absència de parts addicionals (diferents del pagador i el receptor) durant el pagament divideix els sistemes en en línia i fora de línia. Més endavant es veurà que l'absència de terceres parts durant la fase de pagament es considera una característica desitjable.

Finalment, també es podria fer una classificació en funció del moment en el qual es fa la transferència real dels diners. Amb aquesta classificació podríem dividir els sistemes en sistemes a crèdit, sistemes de pagament instantani i sistemes de pre-pagament.

Una possible divisió dels sistemes de pagament electrònic distingeix quatre grups:

1) Xecs electrònics. Els xecs electrònics, substituts dels xecs de paper, proporcionen un mecanisme per a realitzar una transferència de fons entre el compte

bancari del pagador i el compte bancari del receptor. Un xec electrònic és un missatge amb una signatura digital, representant un valor monetari, que es fa efectiu a través d'una tercera part. En aquest tipus de pagaments es fa ús de les xarxes interbancàries existents.

2) Moneda electrònica. Aquesta alternativa emula les característiques de la moneda física. L'anonimat és la seva característica diferenciadora, ja que es pretén que la moneda electrònica permeti realitzar pagaments que no quedin registrats i no vinculin als usuaris amb les seves compres. Altres característiques que s'intenten aconseguir són la transferència fora de línia, la transferibilitat i la seguretat enfront de la falsificació o de l'ús de la moneda en més d'un pagament.

3) Targeta de crèdit. En els pagaments on la targeta de crèdit està present es poden realitzar verificacions en línia durant les transaccions. Per altra part, la utilització de targetes de crèdit sense la presència física del pagador (i per tant de la seva targeta), ja sigui en comandes telefòniques, per correu, o en comerç electrònic, presenta el problema de la identificació de l'usuari, ja que no es pot realitzar la verificació de la targeta ni de la signatura manuscrita de l'usuari. En els sistemes de pagament electrònic mitjançant targeta de crèdit, els receptors es poden posar en contacte amb el banc per a verificar la disponibilitat de fons, però normalment no es realitza la verificació de la identitat de l'usuari, permetent el pagament amb la introducció del nombre de la targeta i la seva data de caducitat, únicament. El protocol SET es va proposar com a protocol de pagament que utilitza les targetes de crèdit tradicionals com a mitjà de pagament substituint les mesures de seguretat físiques per altres de criptogràfiques (com la signatura electrònica) que permeten la identificació del titular de la targeta. L'autenticació de l'usuari també es pot realitzar enfront de la seva entitat bancària o enfront de l'entitat emissora de la targeta utilitzant tècniques diverses (via telefònica, introducció de pin,...). A diferència de la moneda electrònica, que pot ser anònima, les targetes de crèdit identifiquen al seu propietari, i a més els pagaments es poden vincular entre ells.

4) Micropagaments. Els micropagaments es dissenyen especialment per a reduir els costos de comunicació, emmagatzemament i processament relacionats amb el pagament. D'aquesta manera el límit inferior que permet un sistema de micropagament s'adapta a les compres més petites. Aquests pagaments, en ser de petites quantitats permeten relaxar les mesures de seguretat, ja que els riscos estan més controlats. En la majoria de sistemes de micropagament l'anonimat de l'usuari que realitza el pagament se sacrifica per a reduir costos.

2. Sistemes de pagament mitjançant targeta de crèdit

Els sistemes de pagament actuals són molt semblants als sistemes que s'utilitzaven fa algunes dècades, quan les transaccions es realitzaven cara a cara. En l'entorn del món real, el possible frau associat a aquests tipus de pagament es pot mitigar mitjançant polítiques d'ús, mecanismes de seguretat físics o control d'infraestructures. En les transaccions on la targeta no es presenta físicament apareixen noves maneres de cometre frau.

Per tal de dur a terme un pagament segur i confiable utilitzant targetes, s'han de tenir en compte una sèrie de propietats:

- Validesa de la targeta. S'ha de comprovar que la targeta presentada és un mitjà de pagament vàlid.

- Autenticació del propietari. L'usuari que presenta la targeta per a realitzar el pagament n'ha de ser el legítim propietari.

- Confidencialitat. Els detalls del pagament utilitzats en la transacció no han d'estar a la disposició de cap tercera part.

- Privacitat. Les dades de pagament i de la targeta, així com la relació entre la identitat del propietari i una compra, no ha de ser utilitzada per parts no autoritzades ni per propòsits diferents a la mateixa compra.

- Efectivitat. El cost associat a l'ús del mecanisme de pagament, mitjançant targeta ha de permetre que el pagament sigui efectiu i viable.

En els pagaments en el món real l'autenticació de la targeta es realitza segons característiques físiques d'aquesta, com hologrames, bandes magnètiques, etc. L'autenticació del propietari es realitza mitjançant la comprovació de la signatura, de la fotografia o presentant un document acreditatiu.

Quan els pagaments es fan en mode no presencial, l'autenticació s'ha de realitzar utilitzant altres mètodes, el més senzill dels quals és la presentació de dades addicionals al número de targeta, com puguin ser el codi de seguretat, la data de caducitat o l'adreça postal associada a la targeta.

El protocol SSL estableix un canal de comunicació segur entre dos ordinadors. Els usuaris podran intercanviar dades de manera segura així com opcionalment, autenticar-se mútuament. En les operacions de comerç electrònic, habitualment el comerciant s'autentica enfront del consumidor, però aquest darrer

no està obligat a fer-ho. La utilització de SSL en les operacions de pagament mitjançant targeta de crèdit permet que les dades associades al pagament, com el nombre de targeta, es transmetin de manera segura, obtenint confidencialitat. Tot i això, els pagaments utilitzant SSL encara pateixen la mancança d'autenticació del propietari de la targeta. Tampoc permet controlar l'ús que el comerciant fa de les dades de pagament rebudes, obligant el pagador a confiar en el comerciant. Tot i aquests problemes, SSL és amplament utilitzat en els pagments actuals.

Solucionar el problema del coneixement de les dades de pagament per part del comerciant és possible utilitzant SET. SET és un protocol que va ser desenvolupat per Visa i Mastercard per a permetre transaccions electròniques segures. SET permet l'autentició dels dos actors del pagament. Gràcies a la utilització de signatures duals, SET permetia que només l'entitat de pagament pogués veure la informació de pagament associada a l'operació de compra al mateix temps que només el comerciant pogués veure l'ordre de compra. Les característiques de SET i de la signatura dual permeten que el comerciant pugui confiar en l'execució del pagament tot i no conèixer les dades de pagament. Tot i presentar una bona sol·lució als problemes dels pagaments amb targeta de crèdit SET va fracassar. Probablement el fet de requerir l'autenticació del comprador i la necessitat d'aquest d'adquirir un certificat digital va ser determinant.

Signatura dual

La signatura dual vincula dos missatges que s'enviaran a dos destinataris diferents. Cada receptor rebrà una signatura sobre la concatenació dels resums dels dos missatges, així com el missatge que li correspon. D'aquesta manera no podrà coneixer els continguts del segon missatge però si demostrar-ne la vinculació.

Actualment els sistemes de pagament basats en l'entorn dels tres dominis permeten millorar la fase d'autenticació de l'usuari respecte a l'ús de SSL, tot i que sense la necessitat de certificats digitals i per tant mantenint la facilitat dús. En el 3D Secure els usuaris hauran de superar una fase d'autenticació en el moment d'utilitzar la targeta de crèdit en un establiment virtual. El mecanisme utilitzat depèn de l'entitat bancària i de l'emissor de la targeta. Es poden trobar mecanismes d'autenticació que requereixen la introducció d'un pin o una contrasenya associada a la targeta i d'altres una mica més complexos com la utilització de targetes de coordenades o l'enviament d'un codi al telèfon de l'usuari legítim.

3. Sistemes de pagament mitjançant moneda electrònica

La moneda electrònica, també anomenada moneda digital, és el substitut electrònic de la moneda física.

3.1. Característiques ideals dels sistemes de pagament amb moneda electrònica

Entre les característiques de la moneda física es destaquen:

- **És transferible.** El valor de la moneda es troba en ella mateixa, i per tant la transferència de la moneda entre usuaris representa la transferència del valor. A més, les monedes es poden utilitzar en successius pagaments sense necessitat de dipositar-les al banc. El receptor de la moneda té, per tant, la possibilitat d'utilitzar-la en un nou pagament.

- **És infalsificable.** La moneda es crea basant-se en criteris de seguretat que fan difícil la seva falsificació i que permeten la identificació de les còpies falses. Aquestes mesures de seguretat es basen en característiques físiques difícils d'imitar, que limiten la seva reproducció.

- **És anònima.** Les transaccions amb moneda física no requereixen la identificació del pagador ni del receptor del pagament. Si no hi ha altres documents que certifiquin l'intercanvi, la transacció de la moneda física no vincula les identitats dels usuaris.

- **És independent de terceres parts durant el pagament.** Els usuaris pagador i receptor són els únics involucrats en l'etapa de pagament. La seguretat en la validesa de la moneda física fa que no es requereixi la presència de cap tercera part per a validar la transferència.

Les característiques ideals d'un sistema de pagament amb moneda electrònica són aquelles que permeten realitzar transaccions remotes amb les prestacions de les transaccions amb moneda física.

Les característiques ideals de la moneda electrònica tindran com a punt de partida les característiques anteriors. A aquestes característiques se n'hi afegiran altres d'específiques, derivades de la natura digital de les monedes.

1) Independència. La seguretat de les monedes no ha de dependre de cap característica física. Han de ser transmissibles a través de xarxes. Les monedes són una cadena de bits.

2) Seguretat. S'ha de prevenir la creació de monedes falses. D'altra banda, també s'ha de prevenir (o bé detectar) l'ús de còpies de les monedes existents en pagaments (a aquest frau se l'anomena reutilització).

3) Privacitat. Els pagaments han de ser anònims, la identitat del pagador no ha de formar part del pagament, ni de la moneda. No haurà de ser possible establir una connexió entre el pagador i les seves compres encara que més d'una part col·labori (característica coneguda com no rastrejabilitat) així com tampoc vincular, entre elles, les compres realitzades pel mateix usuari (no vinculabilitat).

4) Pagament fora de línia. En un pagament fora de línia (en oposició a en línia), la connexió amb l'emissor de les monedes, amb la finalitat de validació del pagament, no és necessària durant una transferència de pagament. Només intervenen els usuaris pagador i receptor.

5) Transferibilitat. Un sistema transferible presenta la capacitat d'utilitzar la mateixa moneda en transaccions successives sense dipositar-la i sense la intervenció de cap tercera part. Aquesta propietat possibilita que un receptor pugui utilitzar una moneda rebuda per a realitzar un nou pagament.

6) Divisibilitat. La divisibilitat és la capacitat de fraccionar la moneda, i per tant d'utilitzar diferents fraccions de la moneda en diferents pagaments, permetent així pagaments exactes amb fraccions o sumes de fraccions que equivalguin a l'import del pagament. La divisibilitat de la moneda és l'alternativa a la vinculació de diferents monedes en el mateix pagament. Permet obtenir parts de la moneda de manera que la suma de les parts sigui igual al valor de la moneda original. Alguns sistemes que no presenten la característica de divisibilitat implementen la possibilitat de tornar canvi quan el pagament no és exacte.

Aquestes característiques ideals són el punt de partida dels sistemes de pagament mitjançant moneda electrònica. La importància relativa de cada una d'elles dins del conjunt es fixa en funció de l'aplicació. A més, els sistemes de pagament destinats a realitzar pagaments en els quals la quantitat involucrada és fora d'un rang de valors determinat, ja sigui perquè el valor del pagament és molt gran o molt petit es consideraran sistemes de pagament específics, i en aquests casos es fa necessària la redefinició de les característiques ideals.

3.2. Funcionament bàsic d'un sistema de pagament amb moneda electrònica: entitats i procediments

En la seva forma més simple, un sistema de pagament amb moneda electrònica consisteix en un conjunt de quatre procediments que involucren tres parts: el pagador, el receptor i el banc (o bancs, en cas que hi hagi diferents entitats bancàries, i pagador i receptor tinguin comptes en diferents entitats).

Els procediments són:

- **Establiment del compte**. Aquesta operació es realitza una sola vegada. En aquesta etapa es vincula la identitat o el pseudònim de l'usuari al nou compte. L'usuari disposa d'un parell de claus corresponents a un criptosistema asimètric i d'un certificat de clau pública. Determinades operacions sobre aquest compte requeriran el coneixement de la clau privada del parell associat al certificat de l'usuari.

- **Obtenció de la moneda**. Per a obtenir la moneda es poden distingir diverses situacions en funció de si la moneda s'extreu del compte de l'usuari abans del pagament o posteriorment. En el primer cas es disposa d'un sistema de prepagament o a dèbit, mentre que, en el segon, el sistema funciona a crèdit. En un sistema de dèbit el valor és descomptat abans de la seva utilització en l'etapa de pagament. El descompte i la creació de la moneda es produeixen durant l'execució del procediment de reintegrament o retirada (aquest procediment requereix l'autenticació de l'usuari).

- **Pagament**. El pagador duu a terme un pagament involucrant una o més monedes. En determinats sistemes, aquestes monedes són comprovades pel banc en la mateixa fase de pagament. En d'altres, el pagament només conté la transferència de la moneda entre pagador i receptor. En aquest segon cas el receptor podrà comprovar si la moneda és vàlida però no podrà verificar si és la còpia d'una moneda utilitzada abans en una altra transferència.

- **Dipòsit**. Una vegada realitzat el pagament, l'usuari que l'ha rebut el pot fer efectiu dipositant la moneda en el seu compte, encara que en sistemes transferibles també pot optar per transferir la moneda. Si la reutilització de la moneda no ha estat comprovada abans es fa en aquesta etapa. També es comprova que el receptor del pagament no dipositi dues vegades la mateixa moneda.

Sistema a crèdit

L'etapa d'obtenció de la moneda no existeix en sistemes a crèdit, com es diu a R. Rivest, A. Shamir: Payword and Micromint: two simple micropayment schemes, Fourth Cambridge Workshop on Security Protocols, LNCS 1189, pàg. 69-87, Springer Verlag, 1996. En aquest cas la identificació del compte del pagador es fa durant el dipòsit.

3.3. Seguretat en sistemes de moneda electrònica

Els sistemes de pagament mitjançant moneda electrònica inclouen mecanismes de seguretat per tal d'evitar el frau relacionat amb la falsificació i l'ús fraudulent de les monedes. Concretament, els sistemes prevenen o detecten els tipus de frau següents:

- **Falsificació.** La creació de monedes és un dret exclusiu d'alguna de les parts del sistema (per exemple, el banc). Habitualment, els sistemes de moneda electrònica utilitzen protocols en els quals la creació de la moneda involucra el coneixement d'algun paràmetre secret que impossibilita la creació de monedes per parts no autoritzades (falsificació) que no coneixen el paràmetre requerit per a la creació de monedes. Una estructura freqüent consisteix a incorporar a la moneda una signatura digital de l'entitat emissora.

- **Reutilització**. Encara que les monedes digitals no puguin ser falsificades (és a dir, no es poden crear monedes falses diferents de les reals), la duplicació de monedes és fàcilment realitzable perquè només es requereix la duplicació de la informació digital que representa la moneda. A diferència de la moneda física, la moneda electrònica es pot reutilitzar. Per aquesta raó, els sistemes de pagament utilitzen algun mecanisme per a prevenir, en el millor dels casos, o com a mínim detectar els casos de reutilització de monedes. El control sobre la reutilització de les monedes no presenta una solució tan satisfactòria com la prevenció de la falsificació, ja que els usuaris poden no disposar d'informació actualitzada sobre l'estat de la moneda. Per aquesta raó, molts sistemes opten per la detecció en lloc de la prevenció. La prevenció és possible utilitzant dispositius resistents a manipulació per a emmagatzemar les monedes ja que aquests dispositius no permeten el pagament amb monedes ja utilitzades. Aquesta solució pot ser eficaç, encara que costosa, ja que obliga tots els usuaris a disposar d'un dispositiu i utilitzar-lo.

  La segona alternativa per a la prevenció de la reutilització consisteix a contactar amb una tercera part (que pot ser un banc) durant cada pagament (sistema en línia). D'aquesta manera la tercera part centralitza el coneixement sobre la utilització de les monedes i pot informar al receptor del pagament sobre la validesa de la moneda amb la qual el pagador intenta pagar-li.

  Si s'opta per no prevenir l'atac, la reutilització d'una moneda en el mateix comerç o la repetició del seu dipòsit en el banc pot ser detectada a l'instant per part del receptor, però no podria ser-ho, per exemple, la reutilització de la moneda en diferents comerços. En aquest cas la reutilització no es detecta fins que els dos receptors decideixen dipositar la moneda. Per funcionalitat, les monedes es creen amb l'objectiu que es puguin utilitzar en pagaments a qualsevol usuari (encara que alguns sistemes de micropagament generen monedes específiques per a receptors amb els quals l'usuari

manté relacions a llarg termini). Si la moneda pot ser utilitzada per a pagaments a diferents receptors, aleshores s'haurà de solucionar el problema de la reutilització.

En els sistemes on els usuaris s'identifiquen durant l'etapa de pagament, en cas de reutilització es pot identificar fàcilment l'usuari infractor.

- **Sobreutilització**. Els sistemes de pagament han de garantir que totes les monedes creades representin diners existents en el compte de l'usuari. És a dir, les monedes representen diners reals.

  Els sistemes a crèdit, en els quals l'usuari és el creador de la moneda, poden patir sobreutilització. Quan la moneda, després del pagament, és dipositada pel receptor, es pot trobar amb falta de fons en el compte del pagador. En els sistemes a dèbit, les mesures adoptades per a la prevenció de la falsificació prevenen la sobreutilització de les monedes.

3.4. Sistemes en línia i fora de línia

En funció del mecanisme utilitzat per a afrontar el problema de la reutilització, els sistemes de pagament poden validar la moneda en el moment de la transferència (sistema en línia) o bé verificar-la en el dipòsit (sistema fora de línia).

En ambdós tipus de sistemes, el primer pas és l'obtenció de la moneda. La transferència entre pagador i receptor, en canvi, dependrà del tipus de sistema. A continuació es descriuen aquestes etapes quan no s'ofereix privacitat, més endavant, s'analitza l'anonimat en els dos tipus de sistemes.

3.4.1. Creació i obtenció de la moneda en un sistema en línia o fora de línia no anònim

En la creació de la moneda i l'obtenció d'aquesta per part de l'usuari, el primer pas consisteix en la sol·licitud d'obtenció enviada per l'usuari al banc. Amb aquesta sol·licitud, l'usuari espera obtenir una moneda a canvi del decrement pel valor de la moneda en el seu compte. Aquesta és una operació en la qual s'ha d'assegurar que el sol·licitant és efectivament el titular del compte. Per aquest motiu la sol·licitud de creació i obtenció de moneda s'envia signada al banc.

A continuació, el banc crea la moneda utilitzant algun paràmetre secret, per exemple signant la moneda fent servir la seva clau privada, per a prevenir la falsificació de monedes. La moneda inclourà el seu valor i pot incloure una data de caducitat.

Finalment, el banc envia la moneda a l'usuari i descompta l'import del compte de l'usuari. El banc està autoritzat a decrementar el compte d'un usuari únicament quan disposa d'una sol·licitud autenticada que l'autoritza a fer-ho. Si aquesta sol·licitud inclou el valor sol·licitat, el banc només pot decrementar el compte de l'usuari en la quantitat indicada. A més, el banc no podrà utilitzar dues vegades la mateixa sol·licitud si hi ha algun paràmetre que identifiqui la sol·licitud (com un número de sèrie).

Amb aquest procediment el banc coneix, a la vegada, la moneda i l'usuari a qui l'ha enviada. Els pagaments realitzats amb la moneda no seran anònims. Es podrà reconèixer l'usuari a partir de la identificació de la moneda, ja que aquesta està directament relacionada amb la identitat o el compte de l'usuari que la va sol·licitar.

3.4.2. Pagament en un sistema en línia no anònim

En els sistemes en línia, i per a prevenir les reutilitzacions, el banc manté una base de dades amb els números de sèrie de les monedes utilitzades. En tots els pagaments, el receptor sol·licita al banc la comprovació de la moneda abans d'acceptar-la. És a dir, es requereix la participació de la tercera part (banc) en l'etapa de pagament. En cas de reutilització (la moneda ja ha estat utilitzada prèviament, i el seu identificador es troba a la llista), es rebutja el pagament. En canvi si la moneda no és a la base de dades en el moment del pagament, el banc permet al receptor acceptar el pagament. En aquest moment la moneda s'incorpora a la base de dades de monedes utilitzades.

3.4.3. Pagament en un sistema fora de línia no anònim

En els sistemes fora de línia no es fa la comprovació de la validesa de la moneda durant el pagament. Els sistemes fora de línia que no utilitzen dispositius resistents a manipulació per a prevenir la reutilització, afronten el problema des de la perspectiva de la detecció i identificació dels reutilitzadors. La infracció es detecta després del segon dipòsit d'una mateixa moneda. El pas següent és la identificació de l'infractor quan la reutilització ja ha esdevingut. La identificació de l'infractor és senzilla si la identitat del pagador està inclosa dins de la informació relacionada amb el pagament, o bé està inclosa dins de la moneda. No és necessari que la identitat del pagador aparegui de manera explícita per a poder realitzar la identificació del reutilitzador, és a dir, no és necessari que aparegui directament el nom de l'usuari o el seu número de compte. Si un usuari amaga la seva identitat darrera d'un pseudònim, la identificació es podrà dur a terme per part de l'entitat emissora del pseudònim, que pot relacionar la informació no identificadora (pseudònim) amb la identitat de l'usuari.

3.5. Privacitat en sistemes de moneda electrònica: anonimat i no-rastrejabilitat

Es considera una característica desitjable de tot sistema de pagament la possibilitat que el pagador romangui anònim enfront del receptor, i un requeriment encara més estricte, que el pagador romangui anònim també enfront de terceres parts i per tant no se'l pugui vincular posteriorment amb la compra realitzada.

Un sistema serà no rastrejable si la confabulació de les restants parts no pot desvetllar la relació entre la identitat de l'usuari pagador i l'ús donat a les monedes electròniques.

Si, encara que no es reveli la identitat de l'usuari, els pagaments fets pel mateix usuari (o la mateixa parella pagador-receptor) es poden vincular, es dirà que el sistema és vinculable.

En un sistema totalment anònim, a més d'ocultar-se la identitat de l'usuari durant el pagament, s'haurien de garantir la no-rastrejabilitat i la no-vinculabilitat. En un sistema vinculable, es corre el perill que la identificació d'un usuari en un únic pagament permeti desvetllar la totalitat dels pagaments realitzats per aquest usuari.

L'ús de pseudònims permet ocultar la identitat a la resta de parts del sistema, excepte a l'emissor de pseudònims. Aquest emissor podria desvetllar la relació entre les identitats i els pseudònims, destruint l'anonimat del sistema.

En els sistemes de moneda electrònica, l'anonimat dependrà entre altres factors, de la tècnica utilitzada en la creació de la moneda. Si durant la creació de la moneda i la seva posterior emissió el banc pot registrar una característica de la moneda com el seu número de sèrie i vincular-la a l'usuari, encara que aquest després no s'identifiqui durant el pagament, el sistema no serà anònim en sentit estricte. Quan el receptor dipositi el pagament, el banc podrà reconèixer la moneda i informar al receptor de quina és la identitat del pagador: en aquest cas el sistema és rastrejable.

Els sistemes no rastrejables utilitzen tècniques de creació de moneda que permeten que el banc emeti monedes vàlides sense conèixer cap característica d'elles que serveixi per a reconèixer-les posteriorment.

Com a conclusió, establim les següents categories d'anonimat de més laxa a més estricta.

- Pseudònims. En els sistemes on s'utilitzen pseudònims, les operacions identificades utilitzen el pseudònim, de manera que no es revela directament la identitat de l'usuari. Totes les operacions realitzades pel mateix usuari utilitzaran el mateix pseudònim i poden ser vinculades. Si es coneix la identitat de l'usuari en una única operació, aquest coneixement permet identificar totes les operacions realitzades per aquest usuari.

- Anonimat rastrejable. En els sistemes anònims rastrejables, la identitat del pagador no apareix en les operacions de pagament, i per tant l'altra part involucrada en la transferència no coneix la identitat del seu interlocutor. Aquesta circumstància canvia quan s'utilitza el coneixement del que disposen dues o més parts (per exemple, el receptor del pagament i el banc que va generar la moneda). Una confabulació de parts pot revelar la identitat de l'usuari que ha participat en un pagament anònim.

- Anonimat no rastrejable. A diferència del cas anterior, en un sistema no rastrejable, l'anonimat no es pot revocar per l'addició dels coneixements dels quals disposen dues o més parts. Un usuari pot realitzar pagaments anònims amb la certesa que no serà identificat a no ser que cometi frau o activitats delictives.

- Anonimat no rastrejable ni vinculable. Amb la propietat de no-rastrejabilitat es garanteix que la identitat dels usuaris no es revelarà. A més, si no és vinculable, el conjunt de les operacions realitzades per un mateix usuari anònim no es poden vincular. La vinculació permetria obtenir el perfil d'usuaris anònims.

  Tot i ser una característica desitjable, només alguns sistemes de pagament amb moneda electrònica permeten que l'usuari realitzi compres de manera totalment anònima.

Un altre aspecte rarament considerat és l'anonimat de l'usuari que actua com a receptor. Cal igualment protegir la intimitat de la part que rep el pagament, i no ha de ser possible determinar les fonts d'ingressos dels usuaris receptors. En l'anonimat del receptor es poden distingir les mateixes categories: l'ús de pseudònims, l'anonimat únicament enfront del pagador (anonimat rastrejable) i l'anonimat que permet que banc i pagador no puguin vincular el receptor i la font dels seus ingressos (anonimat no rastrejable).

3.5.1. Sistema en línia anònim

Signatura cega

La signatura digital cega és un protocol de signatura digital creat per David Chaum que permet a una persona obtenir un misstage signat per una entitat, sense que sigui necessari desvelar-li el contingut del missatge que s'ha de signar.

L'obtenció de la moneda en el sistema en línia anònim és lleugerament diferent que en el sistema en línia identificat. L'alternativa més habitual és l'ús de signatures cegues en el procés de creació de la moneda. D'aquesta manera el banc no reconeix la moneda que ha creat i, encara que en el dipòsit podrà validar la moneda verificant la signatura, no podrà relacionar la moneda amb l'usuari que la va sol·licitar.

3.5.2. Sistema fora de línia anònim

En els sistemes fora de línia anònims, a diferència dels sistemes fora de línia no anònims, la identificació del reutilitzador no es pot fer directament: el pagament es limita a la transmissió d'una moneda anònima. Si s'opta per prevenir la reutilització, un mecanisme consisteix en l'ús de dispositius resistents a manipulació que impedeixen l'ús d'una moneda en diferents pagaments. Aquests dispositius resistents a manipulació fan una prevenció de la reutilització, però la seva incorporació en els sistemes afecta la viabilitat del sistema, ja que implica que cada usuari tingui un dispositiu per a poder efectuar els pagaments.

Si, en canvi, s'opta per la detecció, hi ha diverses solucions per a aconseguir la identificació. La solució adoptada més freqüentment en els sistemes fora de línia anònims (que no utilitzen dispositius resistents a manipulació) és la revocació de l'anonimat en cas de detecció de reutilització. D'aquesta manera el pagador es manté anònim en el cas general, sempre que no es reutilitza la moneda, mentre que en cas de reutilització, dos pagaments diferents es podran utilitzar per a revelar la identitat de l'usuari infractor.

Aquesta identificació és possible gràcies a la inclusió en el protocol de pagament d'una etapa de repte-resposta en la qual el receptor del pagament envia un repte al pagador i espera obtenir una resposta. El repte es forma a partir de dades aleatòries. La resposta es forma a partir d'informació identificadora de l'usuari, però on aquesta es manté oculta. Si es reutilitza la moneda, aleshores els receptors disposaran de dues respostes a dos reptes diferents. Aquestes respostes permetran revelar la informació identificadora del pagador que es mantenia oculta en cada una de les respostes quan aquestes es presentaven de manera separada (Brands, 1993; Chaum, 1988).

La inclusió d'informació personal oculta es pot realitzar mitjançant diferents tècniques. Aquesta informació romandrà oculta i no podrà ser utilitzada per a revocar l'anonimat dels usuaris que facin un ús correcte de les monedes.

Durant la creació de la moneda, l'entitat emissora s'ha d'assegurar que aquesta informació oculta realment està inclosa en la moneda. Posteriorment si es confirma un cas de reutilització es disposarà de suficient informació per a revelar la identitat de l'usuari infractor. Qualsevol altra situació, com un doble dipòsit per part del receptor del pagament, s'ha de detectar (Brands, 1993) i no podrà ser utilitzada per a revocar l'anonimat del pagador.

Mètodes d'identificació

Els mètodes ***cut and choose*** i **single term** permeten incloure en les monedes informació relacionada amb la identitat de l'usuari.

3.5.3. Descripció d'un sistema fora de línia anònim

El sistema de pagaments anònim presentat a Chaum (1988) permet identificar els usuaris en cas de reutilització. El sistema utilitza la signatura RSA per a la creació de les monedes. Aquestes monedes podrien ser de la forma $(x, f(x)^{1/3}$

(mod n)), on n és un valor la factorització del qual és coneguda només pel banc i f és una funció unidireccional adeqüada.

El protocol per a l'expedició i l'ús d'aquests diners es pot resumir de la manera següent:

1) Alice tria els aleatoris x i r, i envia al banc $B = r^3 f(x) (\text{mod } n)$. Alice sol·licita un dòlar al banc.

2) El banc torna l'arrel cúbica de B mòdul n: $r^* f(x)^{1/3} (\text{mod } n)$ i retira un dòlar del seu compte.

3) Alice extreu $C = f(x)^{1/3} (\text{mod } n)$ de B, ja que coneix el valor de r.

4) Per a pagar 1 dòlar a Bob, Alice li dóna el parell $(x, f(x)^{1/3} (\text{mod } n))$

5) Bob immediatament contacta amb el banc, verificant que aquesta moneda electrònica no ha estat dipositada abans.

Tothom pot comprovar fàcilment que la moneda té l'estructura correcta i ha estat signada pel banc, però, el banc no pot vincular aquesta moneda específica al compte d'Alice.

Entre altres avantatges, l'enfocament de la proposta que es desenvoluparà a continuació elimina el requisit que el comerciant s'hagi de comunicar amb el banc durant cada transacció. Si Alice utilitza una moneda un sol cop, la seva privacitat està protegida incondicionalment. Però si Alice reutilitza una moneda, el banc pot rastrejar el seu compte i es pot demostrar que l'ha utilitzat dues vegades. Per a fer-ho el protocol utilitza el mètode *cut & choose*. A continuació es presenta l'esquema bàsic, que garanteix la impossibilitat de rastreig, però permet al banc traçar un reutilitzador.

Monedes no rastrejables

El banc publica inicialment un RSA mòdul n, la factorització del qual es manté en secret i pel qual $\phi(n)$ no té factors petits. El banc també estableix un paràmetre de seguretat k.

Siguin f i g funcions de dos arguments lliures de col·lisions. Alice té un compte bancari numerat u i el banc manté un comptador associat v. $\oplus$ denota una or exclusiva bit a bit i $\|$ denota la concatenació.

OBTENCIÓ: Per a tenir una moneda electrònica, Alice segueix el protocol següent amb el banc:

1) Alice escull a_i, c_i i d_i, $1 \leqslant i \leqslant k$, de manera independent i uniforme a l'atzar a partir dels residus (mod n).

2) Alice forma i envia al banc k candidats encegats (anomenats B).

$$B_i = r_i^3 * f(x_i, y_i) \bmod n \text{ per } 1 \leqslant i \leqslant k,$$

on

$$x_i = g(a_i, c_i)$$

i

$$y_i = g(a_i \oplus (u \| (v+i)), d_i).$$

3) El banc tria a l'atzar un subconjunt de k / 2 candidats encegats $R = i_j$, $1 \leqslant i_j \leqslant k/2$ i el transmet a Alice.

4) Alice mostra els valors de r_i, a_i, c_i, i d_i, per a tots els i de R, i el banc els comprova. Recordeu que $u \| (v + i)$ és conegut pel banc. Per a simplificar la notació suposarem que R = {k/2+1, k/2+2,. ,. , K}.

5) El banc dóna a Alice $\Pi B_i^{1/3}$ per a tots els i que no pertanyen a R, és a dir $\Pi B_i^{1/3}$ mod n per als valors $1 \leqslant i \leqslant k/2$ i carrega un dòlar al compte d'Alice. El banc també incrementa el comptador d'Alice k unitats.

6) Alice llavors pot extreure fàcilment la moneda electrònica

$$C = \Pi f(x_i, y_i)^{1/3} \bmod n \text{ per als valors de i entre 1 i k/2.}$$

Alice reindexa els candidats en C: $f(x_1, y_1) \leqslant f(x_2, y_2) \leqslant \ldots\ldots \leqslant f(x_{k/2}, y_{k/2}))$. Alice també incrementa la seva còpia del comptador, v, k unitats.

Pagament: Per a pagar 1 $ a Bob, Alice i Bob procedeixen de la manera següent:

1) Alice envia a Bob l'element C.

2) Bob tria a l'atzar una cadena binària $z_1, z_2, z_3, \ldots z_{k/2}$.

3) Alícia respon de la següent manera, per tot $1 \leqslant i \leqslant k/2$:

Si $z_i = 1$, llavors Alice envia a Bob a_i, c_i i y_i.
Si $z_i = 0$, llavors Alice envia a Bob x_i, $a_i \oplus (u \| (v+i))$ i d_i.

4) Bob verifica que C és de la forma adequada i que les respostes d'Alice encaixen amb C.

5) Bob després envia C i les respostes d'Alice al banc, que verifica la seva correcció i incrementa el crèdit del seu compte.

El banc ha d'emmagatzemar C, la cadena binària z_i, ..., z_k i els valors de a_i (per $z_i = 1$) i $a_i \oplus (u \| (v+i))$ (per $z_i=0$).

Detecció de reutilització. Si Alice utilitza la mateixa moneda C dues vegades, llavors té una alta probabilitat de ser traçada: amb alta probabilitat, dos botiguers diferents hauran enviat valors binaris complementaris per al menys un bit z_i. El banc pot buscar fàcilment els seus registres per a assegurar-se que C no s'ha utilitzat abans. Si Alice utilitza C dues vegades, llavors, amb alta probabilitat, el banc té tant a_i i $a_i \oplus (u \| (v+i))$. Per tant, el banc pot aïllar u i rastrejar el pagament fins al compte d'Alice.

Un possible problema amb aquest sistema és una confabulació entre Alice i un segon botiguer Charlie. Després de la transacció amb Bob, Alice descriu la transacció a Charlie, i tant Bob com Charlie envien al banc la mateixa informació. El banc sap que amb una probabilitat molt alta un d'ells està mentint, però no té manera de saber qui, i no es pot rastrejar la moneda fins al compte d'Alice.

Mitjançant la fixació del repte de Bob a Alice, però, es pot evitar que aquesta confabulació defraudi el banc. Cada comerciant té una cadena de consulta fixa. Per a evitar la reutilització per part d'Alice de la mateixa moneda part del repte de la mateixa botiga encara ha de ser calculat a l'atzar.

3.6. Control d'anonimat: revocació

La possibilitat d'efectuar pagaments de manera anònima té com a conseqüència la possibilitat de dur a terme activitats il·lícites, ja que l'usuari infractor pot romandre anònim. Entre aquestes activitats hi ha el blanqueig de diners, l'extorsió o xantatge, la venda de productes il·legals i la compra d'aquests productes.

Blanqueig

El blanqueig és possible si un usuari pot amagar l'origen dels seus ingressos i utilitzar-los anònimament.

Compra-venda de productes il·legals

L'anonimat del pagador permet que un usuari pugui adquirir productes il·legals amb la certesa que no serà identificat. De la mateixa manera, l'anonimat del receptor permet la venda d'aquests productes.

Extorsió i xantatge

Un usuari extorsionador pot exigir que se li donin unes determinades monedes que després pugui gastar anònimament.

3.6.1. Tècniques de control d'anonimat

Una vegada s'ha vist que l'anonimat pot donar lloc a activitats il·lícites es qüestiona la seva conveniència. A favor hi ha la protecció de la intimitat de l'usuari pagador i el seu dret a realitzar compres de manera anònima. La contrapartida és la possible proliferació de les activitats il·lícites indicades anteriorment. La solució general és adoptar una política de control d'anonimat. De la mateixa manera que alguns sistemes amb detecció *a posteriori* de la reutilització de la moneda permeten revocar l'anonimat de l'usuari infractor, els sistemes amb control d'anonimat permeten identificar els usuaris només quan es demostra o se sospita que estan involucrats en alguna activitat il·lícita.

La revocació de l'anonimat és realitzada per una tercera part de confiança (TTP) quan es determina que l'usuari ha infringit la llei. En funció del sistema, aquesta tercera part haurà d'estar present en totes les etapes del pagament o serà suficient que participi únicament en algunes d'elles. En sistemes eficients es requereix la participació de la TTP durant la retirada de la moneda, però no durant el pagament, i només se sol·licita la seva participació en cas de necessitat de revocació.

No totes les activitats il·lícites necessiten el mateix tipus d'algorisme de revocació. Per exemple, un cas de xantatge requereix reconèixer la moneda quan aquesta sigui utilitzada en el futur per a revocar la identitat de l'extorsionador. Altres, com el blanqueig, necessiten identificar les fonts d'ingressos de l'usuari inspeccionat.

Basant-se en aquestes dues necessitats es creen els algorismes de seguiment de moneda (*coin tracing*) i de seguiment d'usuari (*owner tracing*).

- *Coin tracing*. Els algorismes de seguiment de moneda permeten, atesa una moneda determinada en la seva creació, seguir el seu rastre. D'aquesta manera es pot identificar un xantatgista trobant la destinació de les monedes que ha rebut com a resultat del xantatge. Quan el xantatgista intenti gastar la moneda (en sistemes transferibles) o dipositar-la, s'iniciarà la seva identificació revocant el seu anonimat.

- *Owner tracing*. Els protocols d'aquest tipus identifiquen el posseïdor d'una determinada moneda després que es realitzi el pagament. Seran útils per a detectar el blanqueig i les compres il·legals ja que permeten identificar l'origen de les monedes dubtoses. El seu objectiu és permetre rastrejar els

pagaments una vegada realitzats. També permet identificar els compradors de productes il·legals una vegada identificat el receptor.

3.6.2. Característiques ideals del control d'anonimat

Les característiques ideals dels sistemes de revocació de l'anonimat es determinen amb criteris d'eficiència i de privacitat, ja que la revocació no hauria de ser possible sense la certesa de la culpabilitat de l'usuari.

- La revocació és una capacitat exclusiva d'una tercera part de confiança (TTP).

  Ni els pagadors, ni els receptors, ni el banc, ni cap combinació d'ells no ha de poder reconèixer una determinada moneda (vinculada amb una operació concreta) o revelar la identitat del propietari si no és en cas de reutilització o d'activitat il·lícita.

- La TTP actua fora de línia.

  Pel mateix motiu que en les característiques ideals generals dels pagaments s'indica que el banc ha d'actuar fora de línia, ara es considera desitjable que la TTP no intervingui en els pagaments ni en l'obtenció de la moneda ni en el seu dipòsit.

- La TTP només actua quan es requereix legalment.

  No es perd l'anonimat en el cas general. Per als usuaris que actuïn correctament el sistema continua essent anònim. Aquests usuaris han de tenir la certesa que no es revelarà la seva identitat. Per aquest motiu s'han de presentar proves o una ordre emesa per una autoritat per a poder iniciar la revocació.

- La capacitat de la TTP pot estar distribuïda entre diferents entitats.

  La confiança dels usuaris en la TTP és un punt crític del sistema. Per aquest motiu es pot decidir distribuir aquesta confiança en un grup de TTP de manera que només la col·laboració de totes elles (o d'un subconjunt) permeti revocar l'anonimat.

4. Sistemes de micropagament

Els sistemes de micropagament s'adapten a les necessitats dels pagaments de quantitats molt petites, i per aquesta raó presenten una sèrie de característiques diferenciadores dels sistemes de pagament mitjançant moneda electrònica pensats per a pagaments de quantitats majors.

4.1. Motivacions

Les aplicacions recents del comerç electrònic presenten un repte per als sistemes de pagament electrònic existents. Les vendes que involucren el pagament de petites quantitats i les vendes de productes que es poden servir a través de la xarxa presenten característiques especials que la majoria de sistemes de pagament no poden satisfer. El motiu es troba en el marge de benefici del pagament d'una quantitat petita. Aquest no permet utilitzar sistemes on el cost associat es pugui acostar a aquest marge, o fins i tot superar-lo. Els sistemes de micropagament s'adapten als requeriments dels pagaments de petites quantitats, en especial al requeriment d'eficiència que permet costos associats reduïts.

Els micropagaments són especialment útils en la compra d'informació. La informació és un bé que es pot servir a través de la xarxa, és a dir, permet fer un intercanvi instantani entre el bé i la moneda electrònica. La informació es pot vendre en diferents volums, per tant s'haurà de facilitar la compra i el pagament de petites fraccions d'informació. Les monedes electròniques permetrien fer pagaments de quantitats d'informació moderades a grans, però els seus costos associats farien poc viable la compra de petits volums d'informació. Per exemple, es pot utilitzar una moneda electrònica per a pagar la visualització de l'edició electrònica d'un diari complet, però no per a pagar la visualització d'un article concret d'aquest diari, amb un cost molt menor. El preu d'aquest article podria estar per sota del cost mínim per transferència associat al sistema de pagament amb moneda electrònica.

A més, s'ha de tenir en compte que la possibilitat de servir el producte en línia elimina els costos logístics i permet vendre a un preu inferior. Entre els serveis oferts actualment hi ha múltiples aplicacions de la compra d'informació, com ara: visualització de continguts de pàgines web, compres d'arxius musicals, accés a articles de premsa, consultes d'enciclopèdies, descàrrega de programaris de prova, accés a arxius de fotos, mapes o directoris telefònics, consultes en cercadors...

4.2. Alternatives als micropagaments

Actualment, i fins que es generalitzi l'ús dels micropagaments, la informació se serveix utilitzant alternatives al pagament exacte i instantani de la informació consumida. Entre aquestes alternatives trobem:

1) Accés gratuït a la informació. La primera alternativa consisteix a publicar la informació permetent un accés gratuït a aquesta. Aquesta alternativa no presenta una solució general, ja que els posseïdors dels drets de propietat intel·lectual de determinats recursos estan poc motivats a fer-los accessibles d'aquesta manera. D'aquí es deriva que part d'aquests recursos no estiguin disponibles per al seu consum en línia.

2) Publicitat com a font d'ingressos. Després de l'accés gratuït, sense beneficis per al propietari, una altra alternativa àmpliament utilitzada consisteix a obtenir una font d'ingressos (que subvencioni la publicació de la informació) diferent de l'usuari que la consumeix. Les barres publicitàries s'insereixen en els documents que contenen la informació o en permeten la descàrrega. L'empresa anunciadora fa el pagament que permetrà l'accés gratuït a la informació a canvi de la visualització de la publicitat. Algunes de les implementacions d'aquesta alternativa presenten problemes respecte a la protecció de la intimitat dels usuaris, ja que les empreses anunciadores o les empreses que gestionen la publicitat de tercers utilitzen tècniques per a la personalització de la publicitat que rep l'usuari, basant-se en informació recollida dels seus hàbits de navegació.

3) Subscripcions. La tercera possibilitat consisteix a pagar per un volum d'informació gran, que s'anirà consumint amb el temps, és a dir, una subscripció. Podem trobar dos tipus de subscripcions: subscripcions temporals i per accessos. Una subscripció temporal permet l'accés de l'usuari a la informació durant un període de temps determinat. A diferència de la subscripció temporal, una subscripció per volum d'informació permetrà a l'usuari accedir a informació mentre tingui crèdit amb la font d'informació, procedent del pagament inicial. El crèdit inicial s'anirà decrementant en cada accés, independentment del moment que aquest es faci.

Cap d'aquestes alternatives és ideal, ni per a l'usuari, ni per al propietari de la informació. Les dues primeres alternatives permeten a l'usuari accedir gratuïtament a la informació, però no permeten al propietari de la informació cobrar pel volum d'informació consumida. D'altra banda, les subscripcions obliguen l'usuari a pagar per un volum d'informació que potser no arribarà a consumir, i a fer una inversió inicial. Des del punt de vista de l'usuari, realitzar el pagament de la quantitat precisa que es consumeix és la millor alternativa.

4.3. Característiques ideals dels sistemes de micropagament

Les característiques ideals dels sistemes de micropagament difereixen, en part, de les considerades ideals per als sistemes de macropagament. Les característiques ideals dels micropagaments són:

- **Costos per transferència reduïts**. El cost de les microtransferències haurà de representar una petita fracció del valor involucrat en el pagament. Aquest és un requeriment molt exigent en els micropagaments. El seu compliment té com a contrapartida, habitualment, la relaxació o l'incompliment de les altres característiques ideals.

- **Límit inferior**. El límit inferior haurà de ser suficientment petit per a permetre transferències de l'ordre d'un cèntim d'euro per a adaptar-se als pagaments per petits volums d'informació.

- **Control de riscos financers**. En els micropagaments, els mecanismes de seguretat utilitzats per a evitar el frau es limiten per a garantir l'eficiència i mantenir els costos per transferència en un nivell acceptable. La reducció dels mecanismes de seguretat comporta l'aparició de certs riscos financers. Els riscos assumits per qualsevol sistema de micropagament s'han de mantenir controlats i limitats.

- **Intercanvi atòmic**. En la compra dels béns que es poden servir a través de la xarxa, és desitjable la realització del pagament de manera atòmica amb la transferència del bé, de manera que l'intercanvi sigui equitatiu.

- **Velocitat**. La transferència ha de ser prou ràpida per a adaptar-se al microcomerç i per a permetre un gran nombre d'operacions per sessió amb el servidor.

- **Privacitat**. La protecció de la intimitat es considera una característica ideal per a qualsevol sistema de pagament. En general, però, els aspectes relacionats amb la privacitat s'oposen a l'eficiència. Aquest fet és especialment important en els sistemes de micropagament a causa dels alts requeriments d'eficiència que aquests tenen.

4.4. Necessitat de reducció dels costos

L'eficiència en els micropagaments que ens permetrà acceptar pagaments per quantitats molt petites, s'obté reduint els costos associats al pagament ocasionats per diferents factors.

Els costos es poden relacionar amb:

- Costos de control de riscos financers: mesures de seguretat utilitzades per a combatre el frau.

- Costos de comunicació: nombre d'interaccions i volum d'informació transferida.
- Costos de processament de dades.
- Costos relacionats amb l'ús que es dóna a la moneda: moneda genèrica o específica.
- Costos d'emmagatzematge.
- Costos de manteniment de privacitat i anonimat.
- Costos derivats de l'ús de dispositius resistents a manipulació.

Aquesta reducció de costos es pot concretar en quatre punts:

A. Eliminar computació en línia

En els sistemes de pagament electrònic, l'etapa de pagament es pot realitzar amb la intervenció del banc o sense ella. Eliminant la vinculació del banc en l'etapa de pagament es redueix el cost de comunicació. D'altra banda els sistemes fora de línia permeten transferències més ràpides i amb menys operacions. Com a contrapartida, els sistemes fora de línia poden patir reutilització. La prevenció de la reutilització de monedes es podria realitzar amb l'ús de dispositius resistents a manipulació, com són les targetes intel·ligents. Encara que les targetes intel·ligents poden fer les funcions del banc de manera distribuïda, es descarta el seu ús en els micropagaments ja que introdueixen el cost addicional del seu manteniment. Per aquest motiu els sistemes de micropagament tendeixen a introduir l'ús de moneda específica com a mesura de prevenció de la reutilització.

B. Minimització de l'ús de criptografia asimètrica

En els sistemes de pagament amb moneda electrònica, la criptografia asimètrica es combina amb la criptografia simètrica i les funcions de *hash*. La criptografia asimètrica permet realitzar tasques d'identificació i autenticació d'usuaris. La creació de monedes (per part del banc en els sistemes a dèbit) implica en bona part dels casos l'ús de criptografia asimètrica. En considerar l'ús d'aquestes funcions en els sistemes de micropagament trobem uns costos associats elevats. Aquests costos són de tipus diferents i són provocats per diferents causes.

Ús de certificats: la verificació de signatures, així com altres operacions realitzades amb criptografia asimètrica, requereixen l'ús del corresponent certificat de clau pública. Els certificats han de ser emesos per una tercera part de confiança i renovats periòdicament. També s'han de gestionar les llistes de revocació dels certificats.

Computació intensiva: els algorismes d'encriptació i desencriptació dels criptosistemes de clau pública tenen un cost computacional superior al dels algorismes de clau secreta. Encara així, la criptografia asimètrica no desapareix en tots els sistemes de micropagament. En els que es manté, les costoses ope-

racions s'amortitzen sobre diversos micropagaments per a distribuir el cost computacional i mantenir-lo limitat.

C. Suprimir l'anonimat i la privacitat

Els sistemes anònims utilitzen majoritàriament criptografia asimètrica. En el punt anterior es descriuen les causes que fan recomanable la minimització de l'ús de la criptografia asimètrica. Amb l'objectiu de minimitzar les operacions realitzades amb criptografia asimètrica, l'anonimat es considera una característica prescindible, en favor de l'eficiència. Normalment no s'inclou anonimat en els sistemes per a micropagaments. En els sistemes en què es considera l'anonimat, el cost computacional corresponent a cada pagament s'acosta al cost dels pagaments amb moneda electrònica fent-lo no factible per a la seva utilització en micropagaments.

D. Ús de moneda específica

Les monedes específiques només poden ser utilitzades amb un receptor determinat. Vinculen tant l'emissor com el receptor del pagament (en determinats casos només vinculen el receptor) i suposen l'establiment de relacions a llarg termini, ja que la generació eficient de moneda específica es basa en la creació de conjunts de monedes que seran utilitzades per a pagaments al mateix receptor.

4.5. Descripció d'un sistema de micropagament

En aquesta secció es descriurà un sistema de micropagament: el sistema payword descrit Rivest i Shamir (1996).

Payword és un sistema de micropagament on les parts són brokers, usuaris pagadors i venedors o proveïdors. Els brokers autoritzen els usuaris a realitzar micropagaments i accepten els pagaments rebuts pels venedors. El broker manté relacions a llarg termini amb usuaris i venedors.

Payword és un sistema basat en crèdit i optimitzat per seqüències de micropagaments. El seu funcionament es basa en les fases següents

1) Un usuari crea un compte amb un broker, que proporciona a l'usuari un certificat signat digitalment. Aquest certificat autoritza l'usuari a fer cadenes de paywords, que són cadenes de valors de *hash*.

2) Abans de contactar amb un proveïdor o venendor, l'usuari crea fora de línia una cadena de paywords específica del seu proveïdor.

3) L'usuari autentica la cadena completa al proveïdor amb una sola signatura amb un sistema de clau pública, i després, successivament, revela cada payword de la cadena per fer cada micropagament.

4) El venedor cobra els paywords rebuts de l'usuari amb el broker original.

Cadenes de paywords

En la construcció d'una cadena payword, s'utilitza una funció *hash* unidireccional, tal com MD5. La funció de *hash* h té la propietat que, donat un valor y, és difícil trobar una entrada x, tal que y = h (x).

Un usuari crea una cadena payword $\{W_0, w_1, w_2, ..., w_n\}$ escollint el payword final w_n a l'atzar i calculant els altres paywords a través de la funció de *hash* $w_i = h\ (w(i+1))$. El primer payword w_0 s'anomena l'arrel de la cadena. Donat w_0 és difícil per a qualsevol persona que no sigui l'usuari calcular la resta dels paywords de la cadena.

Relació usuari-broker

Un usuari inicia una relació amb un broker en sol·licitar un compte i un certificat payword. L'usuari dóna primer mitjançant una connexió segura autenticada: el seu número de targeta de crèdit, la seva clau pública PK_U, i la seva "adreça de lliurament" (per exemple, adreça IP). El broker, a continuació, emet un certificat signat digitalment que autoritza l'usuari a fer cadenes payword fins a una data de venciment determinada, i autoritza el lliurament de béns només a l'adreça de lliurament especificada.

El certificat d'usuari, C_U té la forma següent: C_U = { broker, usuari, adreça de lliurament de l'usuari, PK_U, data d'expiració, altre informació} $_{SKB}$, on SK_B denota que el contingut de {} està signat amb la clau privada del broker, SK_B.

El certificat C_U és una declaració del broker per a qualsevol proveïdor que autentica els paywords produïts per l'usuari i que siguin utilitzats abans de la data de venciment, assegurant el seu cobrament.

Relacició usuari-venedor

Les relacions entre l'usuari i el venedor són transitòries. Un usuari podria visitar un lloc web, comprar deu pàgines, i després passar a comprar en altres llocs. Quan l'usuari contacta amb un nou proveïdor, calcula una nova cadena payword $\{W_0, w_1, w_2, ..., w_n\}$. Aquí el valor de n es tria segons la conveniència de l'usuari; podria ser deu o deu mil.

A continuació, l'usuari calcula el seu compromís per a la cadena: M = {venedor, C_U, W_0, data actual, altres informacions} $_{SKU}$.

El compromís M, que se signa amb la clau privada de l'usuari SK_U, autoritza el broker a pagar el venedor per qualsevol dels paywords w_1, w_2, ..., w_n.

Els paywords són específics del seu proveïdor i específics de l'usuari que els ha creat; no són de cap valor per a un altre proveïdor. En rebre el compromís M, el proveïdor verifica la signatura de l'usuari a M i la signatura del broker a C_U (contingut dins M), i comprova la data de venciment. A més del compromís, el pagament d'un usuari a un proveïdor consta d'un payword i el seu índex: (w_i, i). El pagament no està signat per l'usuari.

L'usuari passa els seus paywords en ordre: w_1 primer, i després w_2, i així successivament. Si cada payword val un cèntim i cada pàgina web costa un cèntim, dóna a conèixer al proveïdor w_i en demanar la seva i-èssima pàgina web del proveïdor d'aquest dia.

Això condueix a la política de pagament payWord: per a cada compromís al venedor se li paga 1 cèntim essent (w_L, L) el pagament rebut amb un major índex. Això significa que el proveïdor necessita emmagatzemar un sol pagament de cada usuari: el que té l'índex més alt. El broker pot determinar el valor a ser pagat per w_L determinant quantes vegades s'ha d'aplicar la funció de *hash* h sobre w_L per a obtenir W_0.

Relació venedor-broker

Un venedor o proveïdor no necessita tenir una relació anterior amb un broker, però necessita obtenir la clau pública del broker d'una manera autenticada, per a poder autenticar certificats signats pel broker. També necessita establir una manera per tal què el broker li pagui els paywords rebuts.

Al final de cada dia (o del període adequat), el proveïdor envia un missatge al broker per a cada un dels usuaris del broker que ha pagat al proveïdor aquest dia, els compromisos C_U i l'últim pagament P = (w_L, L). El broker necessita primer verificar cada compromís rebut comprovant les signatures dels usuaris. A continuació, comprova cada pagament (w_L, L) aplicant la funció de *hash* L vegades.

5. Característiques addicionals: transferibilitat i atomicitat

En aquest capítol es presenten dues característiques addicionals que permetrien dotar els sistemes de pagament de més prestacions. Es tracta de la transferibilitat i l'atomicitat.

5.1. Transferibilitat en sistemes de moneda electrònica

La transferibilitat és una de les característiques de la moneda física i, per tant, una característica desitjable en els sistemes de moneda electrònica.

En els sistemes transferibles, les monedes poden ser transferides múltiples vegades entre usuaris, sense la necessitat d'una verificació en línia per part d'una tercera part de confiança, i sense haver de ser dipositades.

Es pot dir que la transferibilitat és la generalització del pagament fora de línia, ja que un protocol transferible conté els mateixos subprotocols que un protocol fora de línia, amb la diferència que el subprotocol de transferència o pagament es pot executar múltiples vegades entre la retirada i el dipòsit.

La solució al problema de la reutilització, adoptada en molts sistemes fora de línia anònims, és la d'incloure en els pagaments alguna informació sobre el pagador. Aquests sistemes permeten les reutilitzacions en l'etapa de pagament, i les detecten més tard durant el dipòsit de la moneda. Si el pagador usa la moneda només una vegada, la informació d'identificació inclosa en ella no permet fer la identificació, però si es reutilitza la moneda, la informació revelada en dos pagaments es pot emprar per a identificar el reutilitzador. Els sistemes anònims transferibles, com a generalització dels sistemes fora de línia anònims, utilitzaran les mateixes tècniques d'identificació de reutilitzadors, però ara s'aplicaran a tots els usuaris que realitzin pagaments amb la moneda.

5.2. Incorporació d'atomicitat als protocols de pagament electrònic

En una compra electrònica es fa un intercanvi sempre que s'utilitza un mitjà de pagament electrònic a canvi d'un bé o servei adquirit en un establiment electrònic.

Sovint es parla de l'atomicitat com una característica desitjable per als sistemes de pagament electrònic. Possibles fallades de la xarxa per una part, i el comportament fraudulent de qualsevol de les parts involucrades en l'intercanvi per l'altra, poden ocasionar situacions on una de les dues parts proporcioni el bé o realitzi el pagament i no rebi, a canvi, el pagament o el bé de l'altra part. L'atomicitat permet vincular una sèrie d'operacions de manera que s'executin en la seva totalitat o no s'executin en absolut. L'intercanvi atòmic pretén que l'intercanvi es realitzi totalment o no es realitzi, i per tant no hi hagi pèrdues per a cap de les dues parts.

La confiança que un usuari diposita en un servei és fonamental a l'hora de decidir-se a utilitzar-lo. La seguretat que els pagaments realitzats tenen garantida l'entrega del bé, és a dir, l'atomicitat, pot representar un augment en la confiança que la transacció electrònica inspira a l'usuari, que d'altra manera pot no estar disposat a realitzar un pagament sense la certesa de la recepció del producte.

En la compra de béns digitals utilitzant moneda electrònica, tant el bé com la moneda es transmeten en línia, ja que el bé es pot servir electrònicament, i per tant, les parts poden intercanviar directament la moneda electrònica i el bé adquirit, en una operació denominada pagament a canvi d'un producte. Si la compra és d'un bé tangible, i per tant requereix un enviament físic, l'intercanvi no es formalitzarà entre bé i moneda, sinó que l'alternativa és un intercanvi de la moneda per un rebut del pagament. El rebut consistirà en un compromís per part del venedor on es reflecteix l'evidència del pagament i la descripció del bé que serà transferit a través d'un enviament físic. Aquest rebut serà utilitzat com a prova de la conclusió de la compra en cas de disputa.

Les fallades de la xarxa poden donar lloc a situacions on les monedes poden passar a estar en un estat ambigu, on es podria arribar, fins i tot, a perdre el seu valor. Per exemple, en un sistema de moneda electrònica anònima fora de línia amb detecció de reutilització en el qual una errada ocasiona que un pagador no pugui saber si el receptor ha rebut o no la moneda, no es pot arriscar a utilitzar-la de nou ja que si ho fes i el pagament s'havia enllestit, l'usuari no tan sols seria identificat sinó que també seria acusat de reutilització.

Exercicis d'autoavaluació

1. Observeu el funcionament de la fase de pagament de diversos establiments comercials virtuals. Quins sistemes de pagament utilitzen? Descriviu-los.
En el cas de permetre pagaments mitjançant targeta de crèdit, quins mecanismes d'autenticació heu pogut observar?

2. Descriviu el funcionament d'un algorisme concret de signatura cega.
En general, creieu que seria possible realitzar una signatura sobre un conjunt d'informació de la qual una part fos visible (i es pogués verificar) i una altra part fos oculta?

3. És possible fer un sistema de micropagament anònim?
En cas afirmatiu proposeu una tècnica per a fer-ho o descriviu alguna proposta publicada.

Bibliografia

S. Brands, *Untraceable Off-line Cash in Wallets with Observers*, Advances in Cryptology - CRYPTO '93, 1993, pages 302-318.

D. Chaum and A. Fiat and M. Naor, *Untraceable Electronic Cash*, CRYPTO'88: Proceedings on Advances in Cryptology, LNCS 403, 1988, pages 319-327.

Ronald L. Rivest and Adi Shamir, *PayWord and MicroMint: two simple micropayment schemes*, CryptoBytes, 1996, pages 69-87.