SISTEMAS DE PAGOS ELECTRÓNICOS

Josep Pegueroles Vallés

Profesor Asociado del Departamento de Ingeniería Telemática
Universitat Politècnica de Catalunya

josep.pegueroles@entel.upc.es

1. INTRODUCCIÓN.

Inmersos en la denominada Sociedad de la Información, nuestra forma de relacionarnos está cada vez más ligada a las redes de ordenadores y en particular a Internet. La tecnología basada en el uso de computadoras está transformando nuestra forma de acceder, guardar y distribuir la información. Uno de los campos que ya ha sufrido un cambio importante debido a la introducción de estas tecnologías es el comercio.

La realización de transacciones financieras a través de información electrónica sobre líneas de telecomunicaciones es lo que se denomina comúnmente Comercio Electrónico. Un punto clave para el éxito del comercio electrónico es el uso de sistemas de pago seguros y eficientes. La necesidad de seguridad en este tipo de transacciones se ve incrementada si se tiene en cuenta que se estima que la mayoría de dichos intercambios se realizarán a través de Internet (ya sea mediante el uso de ordenadores personales o teléfonos móviles).

Existen distintos sistemas de pago electrónicos: cheques digitales, tarjetas de crédito, tarjetas de débito, tarjetas prepago... Los servicios de seguridad requeridos usualmente para este tipo de sistemas son privacidad (protección frente a escuchas), autenticación (identificación de usuario e integridad del mensaje) y no repudio (protección frente a negaciones de servicio prestado).

El sistema de pago electrónico menos extendido, debido en gran medida a la dificultad de su implementación, es la moneda electrónica o *Electronic cash*. Tal como su nombre indica, los sistemas de moneda electrónica pretenden ofrecer un sistema de pago con las mismas características que presenta la moneda tradicional o papel moneda.

La moneda electrónica deberá ser: universal, es decir, deberá poderse utilizar en cualquier lugar y a través de cualquier medio electrónico; segura, de difícil falsificación y duplicación; anónima, deberá poder utilizarse sin que su propietario sea identificado, de la misma forma que es posible efectuar el pago de servicios o productos mediante la moneda corriente sin que los billetes utilizados puedan por lo general identificar al comprador; autentificable, su validez deberá poder ser comprobada sin necesidad de acudir a una entidad de verificación, de la misma forma que la autenticidad de los billetes en curso puede ser reconocida por lo general sin acudir al banco; transferible, ha de ser posible intercambiar bits de un monedero electrónico a otro, de la misma forma que es posible hacerlo con los billetes; divisible, debe ser posible hacer cambios de un valor a valores inferiores, lo mismo que un billete analógico de un determinado valor es equivalente al conjunto de otros de valor más pequeño.

La mayoría de estudios sobre moneda electrónica se centran en garantizar las características de no trazabilidad y anonimato. En general, los esquemas de moneda electrónica consiguen estos servicios de seguridad mediante el uso de firmas digitales, éstas se podrían considerar como el equivalente digital de las firmas manuscritas.

Las firmas digitales se basan en el uso de criptografía de clave pública. En este tipo de criptosistemas, cada usuario posee un par de claves, una pública y otra privada o secreta. La clave privada se usa para generar las firmas digitales, mientras que la clave pública sirve para verificar dichas firmas. Este mecanismo requiere cierto grado de certeza sobre la propiedad de las claves públicas (un usuario debe estar seguro que la clave pública que usa para verificar al firmante realmente pertenece al firmante), esto introduce un problema de gestión de claves y su solución pasa por crear una cierta infraestructura para la autenticación, esto es, existencia de organismos notarizadores de la propiedad de esas firmas. Además, estos sistemas deben presentar seguridad física y de red suficiente para garantizar la privacidad de las claves secretas.

En este artículo se da una visión general del estado del arte en los mecanismos de pagos electrónicos, haciendo especial hincapié en los sistemas de pagos anónimos y aproximaciones a sistemas de moneda electrónica. En primer lugar se presentan las definiciones de los conceptos y la terminología básica usada en el campo así como los criterios de clasificación más comúnmente usados. Seguidamente se presenta las herramientas básicas usadas para prestar servicios de seguridad a los sistemas de pagos electrónicos. A continuación, partiendo de un modelo clásico sencillo de transacción electrónica segura sin anonimato ni no trazabilidad, se discutirá sus ventajas y carencias, y se irán presentando protocolos más sofisticados para finalmente exponer el modelo que cumpla las características de moneda electrónica. Finalmente se describen a alto nivel algunos de los protocolos propuestos en la

literatura, clasificados según sus características de trazabilidad y on/off-line.

2. DEFINICIONES.

Antes de adentrarnos en los protocolos de pagos electrónicos haremos un breve repaso a la nomenclatura y definiciones más comúnmente usados.

2.1 Comercio Electrónico vs Pagos Electrónicos.

El término Comercio Electrónico se refiere a cualquier transacción financiera que implique transmisión de información de forma electrónica. Los paquetes de información que se transmiten se denominan testigos electrónicos o Electronic tokens. No se debe confundir el testigo, que es una secuencia de bits, con su soporte físico, este soporte físico se denomina comúnmente tarjeta, ya que la mayoría de veces toma la forma de una tarjeta de plástico del tamaño de un monedero (un ejemplo serían las tarjetas de crédito); de cualquier forma también puede ser, por ejemplo, la memoria de un ordenador.

Un caso particular de comercio electrónico es el pago electrónico. Un protocolo de pago electrónico consiste en una serie de transacciones al final de las cuales se ha realizado un pago mediante el uso de un testigo que ha sido acuñado por una entidad autorizada. Para mayor simplicidad consideraremos que dicha entidad autorizada no puede coincidir con el comprador ni el vendedor.

Tal como se ha expuesto, el esquema de un pago electrónico implicará necesariamente el concurso de 3 agentes, véase figura 1:

- Un comprador, aquel que realiza el pago, y que de ahora en adelante llamaremos Alice o Comprador.
- Un vendedor, aquel que recibe el pago, y que de ahora en adelante llamaremos Bob o Vendedor.
- Una entidad financiera, de la cual Alice retira el dinero de su cuenta y a la cual Bob deposita el dinero en su cuenta. A dicha entidad la denominaremos a partir de ahora Banco, y para mayor simplicidad, de momento, sólo consideraremos el caso en que Alice y Bob tienen cuenta en el mismo banco.

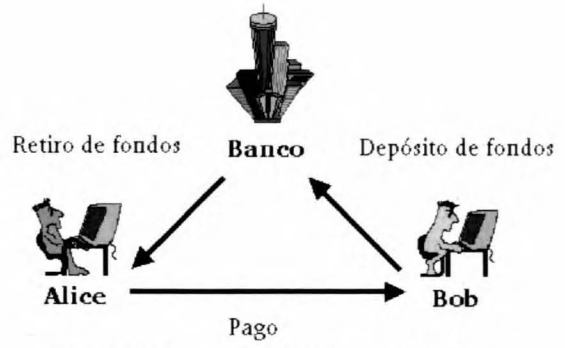

Figura 1. *Esquema básico de pago electrónico*

Adicionalmente, en esquemas más complejos, puede aparecer la figura del intermediario, que se encargaría de funciones propias del Banco, pero lo haría transparente a Comprador y Vendedor. Más adelante nos encargaremos de esta figura.

2.2 Seguridad en los pagos electrónicos.

Los pagos electrónicos, expuestos en el apartado anterior, pueden realizarse a través de medios de transmisión abiertos o cerrados. Con el auge de las telecomunicaciones y el éxito de la red Internet, cada vez es más frecuente que dichas transacciones electrónicas se realicen sobre medios de transmisión inseguros (pensemos que hasta hace muy poco la mayoría de transacciones electrónicas se realizaban a través de EDI sobre circuitos propietarios o mediante líneas dedicadas). Este escenario hace especialmente importante la seguridad de los mensajes que se envían a través de esas redes.

Los servicios básicos de seguridad requeridos para que se confíe en las transacciones económicas sobre este tipo de medios electrónicos son:

- Privacidad, o protección frente a escuchas. Este servicio es especialmente importante para transacciones en las que los números de tarjetas de crédito se envían a través de la red.
- Identificación de usuario o protección frente a suplantación de personalidad. Cualquier intercambio o transacción económica debe asegurar que los participantes en esa transacción sepan con quien están tratando.
- Integridado protección frente a sustitución del mensaje original. Se debe asegurar que la copia del mensaje que se recibe es la misma que la que se envió.
- Repudio, o protección frente a posteriores negaciones de servicio prestado o recibido.

Normalmente, los tres últimos servicios se engloban en un único término: Autenticación. Estos servicios de seguridad se pueden conseguir de muy distintas formas, la técnica más empleada se fundamenta en Infraestructuras de Autenticación.

En dicho esquema, la privacidad se consigue mediante el cifrado del mensaje con una clave secreta conocida únicamente por el emisor y el receptor. La autenticación se consigue mediante sistemas de distribución de claves. Los sistemas de distribución requieren autoridades de certificación, o agentes de confianza que son los responsables de garantizar la identidad de usuario. Cada integrante en una transacción económica debe tener su identidad garantizada (incluyendo los bancos) mediante un certificado. Este certificado se puede usar cada vez que el usuario quiera identificarse frente a otro usuario.

Aunque la infraestructura de autenticación no se puede considerar parte integrante del esquema de comercio electrónico, los servicios de seguridad que proporciona son esenciales en dicho esquema. En todos los modelos

propuestos en este informe se asume la existencia de una infraestructura de autenticación que proporciona dichos servicios, de esta forma, en la exposición de los protocolos, nos centraremos en la parte referida a la transacción.

2.3 Anonimato y concepto de Moneda Electrónica.

Los servicios de seguridad expuestos anteriormente se consideran los mínimos necesarios para depositar confianza en un sistema de pago electrónico pero distan mucho de tener todas las propiedades expuestas por Okamoto en [Oka92].

Pensemos que el término Dinero Electrónico se usa normalmente para designar cualquier tipo de pago electrónico que de alguna manera hace pensar al usuario que dispone de "efectivo", aunque en realidad, dicho término sólo hace referencia a un sistema específico de pago que viene muy acotado por ciertas propiedades criptográficas.

Hasta el momento, dentro de la definición de seguridad, sólo nos hemos referido a la privacidad como protección frente a escuchas, pero existe un concepto mucho más amplio de privacidad, introducido por David Chaum en 1992 [Cha92]. En dicha definición Chaum afirma que no existe privacidad completa mientras las entidades financieras puedan confeccionar historiales de compras susceptibles de ser analizadas no sólo por ellos sino también por el gobierno.

Para conseguir esta privacidad en sentido más amplio, no sólo se requiere el uso de las técnicas tradicionales que proporcionaban protección frente a escuchas sino que además se necesita anonimato en las transacciones.

En particular aparece la necesidad de dos nuevos servicios:

- Anonimato del comprador durante el pago.
- No trazabilidad del pago, de forma que el banco no pueda averiguar "el dinero de quien" se ha usado para realizar un determinado pago.

Las tarjetas de crédito convencionales no proporcionan este tipo de seguridad, por esta razón Chaum introdujo el concepto de Moneda Electrónica, *electronic cash* o *digital cash*, como un sistema de pago electrónico que garantice, además de los servicios básicos expuestos los de anonimato y no trazabilidad antes mencionados. Como también se aprecia en la figura 1, cualquier esquema de pago electrónico debe seguir los siguientes pasos:

- Retiro de fondos o en inglés *withdrawal*. Donde Alice transfiere parte de su dinero desde su cuenta en el banco a una tarjeta propia.
- Pago en donde Alice traspasa el dinero de su tarjeta a la de Bob.
- Depósito de fondos en el cual Bob transfiere el dinero que ha recibido de Alice a su cuenta en el banco.

Estos pasos se pueden realizar de dos distintas formas:

- On-line, si Bob contacta con el banco para verificar la validez del testigo de Alice antes de aceptar el pago y enviarle el producto, es decir, durante el proceso de compra se contacta con el Banco. Este mecanismo es el más usado hoy en día en sistemas basados en tarjeta de crédito.
- Off-line, Bob realiza el depósito del dinero que le ha dado Alice, para que el Banco lo verifique y lo ingrese en su cuenta, cierto tiempo después de que le haya aceptado el dinero y enviado el producto. Es decir, Bob no contacta con el banco durante el proceso de compra-venta.

Existen otras formas de clasificar los pagos electrónicos, atendiendo al momento en que se realiza el retiro de dinero de la cuenta del comprador. En este sentido, los pagos electrónicos se pueden clasificar en:

- Sistemas pre-pago. Si el comprador ve decrementada su cuenta bancaria antes de realizar la compra. Este método se correspondería con los sistemas de monedero electrónico y tarjetas telefónicas. Éste sería el sistema más análogo al papel moneda tradicional.
- Sistemas de pago instantáneo. Cuando al comprador se le realiza el cargo en cuenta justo en el momento de realizar la compra. Se correspondería con los sistemas actuales de pagos con tarjeta de débito (Visa Electron, 6000, ...).
- Sistemas a crédito. Cuando Alice realiza la compra, el Banco asegura al vendedor que se le hará efectiva la cantidad acordada, pero Alice sólo verá decrementada su cuenta cierto tiempo después de haberse realizado la compra.

Otro criterio habitual es la cantidad implicada en la transacción, de esta forma se clasifican los pagos electrónicos como:

- Macropagos, cualquier pago superior a 10 euros.
- Pagos, aquel que la cantidad está comprendida entre 1 y 10 euros.
- Micropagos, cualquier pago inferior a 1 euro.

Los pagos superiores a 10 euros se realizan mayoritariamente entre dos empresas, es por esto que también reciben la denominación global de pagos B2B (*Business to Business*).

Normalmente los pagos inferiores a 10 euros, tanto si son pagos como micropagos, se realizan entre empresa y usuario o entre usuario y usuario, por esto, este tipo de pagos también se denominan B2C (*Business to Consumer*) o C2C (*Consumer to Consumer*) dependiendo del caso. Estos últimos sistemas presentan el problema añadido del coste de implementación, ya que no tendría sentido utilizar un sistema de pago cuyo coste económico sea del orden de magnitud o superior al importe de la transacción.

Finalmente, la prestación o no de los servicios de seguridad añadidos presentados por Chaum en [Cha92] (Anonimato y trazabilidad) también sirven para clasificar los pagos electrónicos como Anónimos o No Anónimos, Trazables o No Trazables.

Atendiendo a estas clasificaciones, el sistema electrónico análogo al papel moneda descrito por Okamoto debería ser Off-line, Pre-pago, Micropago, Anónimo y No trazable.

Llegados a este punto se podría plantear que las características extendidas que serían deseables en un sistema de pago electrónico entran en conflicto con las características básicas que se les pedía a los sistemas de pago electrónicos, la identificación de usuario frente al anonimato, por ejemplo, o el no repudio frente a la trazabilidad.

Una reflexión profunda sobre el significado de dichas características llevaría a la interpretación de los servicios clásicos de Identificación de usuario, Integridad y No Repudio como garantía de legitimidad de usuario. En otras palabras, que garanticen que el participante en la transacción es un individuo autorizado y competente para realizar la transacción, aunque no se sepa realmente quien es. Visto esto, podríamos reformular las características generales de cualquier sistema de pago electrónico como:

- Secreto
- Legítimo

La necesidad de distintas características: Anonimato o Identificación, Trazabilidad o No Repudio, Pagos Grandes o Pagos Pequeños... darán lugar a distintas concreciones de pagos electrónicos, una de las cuales será la Moneda Electrónica.

2.4 Nuevas Amenazas.

La introducción de las nuevas características de anonimato y no trazabilidad que dan lugar al concepto de Moneda Electrónica propician la aparición de nuevas amenazas de uso indebido de la misma que debemos evitar o detectar. Análogamente a lo que ocurre con la falsificación del papel moneda tradicional, existen dos riesgos de uso ilícito en los sistemas de moneda electrónica:

- Falsificación de testigo o *Token forgery*. Que consiste en la creación de una moneda electrónica aparentemente válida sin la realización del correspondiente retiro de fondos.
- Pago múltiple, en inglés *Multiple spending, respending, double spending o repeat spending*. Que consiste en el uso de la misma moneda electrónica para realizar distintos pagos, de modo que un único retiro de fondos cubriría múltiples compras. Esta amenaza toma gran relevancia ya que debe tenerse en cuenta que la moneda electrónica no es más que información digital, y por tanto, reproducible tantas veces como se quiera.

Existen dos filosofías de protección frente a estas amenazas: protección a priori, o intentar prevenir que las amenazas se materialicen en ataques, y a posteriri, que consiste en la posibilidad de detección del ataque y su correspondiente penalización, de esta forma no se toma ninguna medida para que no se realice el ataque, pero se garantiza que un ataque será detectado, y consecuentemente, penalizado.

3 PROTOCOLOS

Seguidamente se presentarán los protocolos genéricos básicos para conseguir los distintos sistemas de pago según las características expuestas en la sección anterior. Partiendo de un modelo clásico sencillo de transacción electrónica segura sin anonimato ni no trazabilidad se irán presentando protocolos más sofisticados para finalmente exponer el modelo que cumpla las características de moneda electrónica.

3.1 Pagos electrónicos trazables.

Los pagos electrónicos trazables son aquellos en que es posible saber qué individuo ha realizado una determinada compra o transacción.

3.1.1 Pago electrónico on-line.

En todos los sistemas on-line la acción de pago y la de depósito coinciden ya que la conexión obligada para la comprobación de la validez del token se aprovecha para ingresar el token en la cuenta del receptor. Los sistemas on-line son los de más fácil solución frente a problemas de *double-spending* pero a su vez son los que generan mayor tráfico en las redes, debido precisamente a la necesidad de realizar una conexión con el Banco para cada realización de pago.

La serie de acciones implicadas en el proceso son las que se describen a continuación.

Retiro de fondos:

```
- Alice envía una petición de retiro de
fondos al Banco.
- El Banco prepara una moneda electrónica y
la firma digitalmente.
- El Banco envía una moneda a Alice y la carga
en su cuenta.
```

Pago y depósito de fondos.

```
- Alice envía la moneda a Bob.
- Bob contacta con el Banco y le envía la
moneda.
- El Banco verifica la firma digital del
Banco.
- El Banco verifica que la moneda no ha sido
ya gastada.
- El Banco consulta su registro de retiro de
fondos para confirmar el retiro de fondos de
Alice (opcional).
- El Banco  introduce la moneda en la base
de datos de monedas gastadas.
- El Banco ingresa la cantidad en la cuenta
de Bob y le informa.
- Bob da a Alice la mercancía.
```

3.1.2 Pago electrónico off-line

Para minimizar la cantidad de tráfico generado en la red de los sistemas on-line se propusieron sistemas fuera de conexión u off-line. En ellos no es necesaria la conexión con el Banco para cada transacción pero es preciso utilizar mecanismos mucho más robustos de detección de doble uso, ya que el uso de la moneda sólo se podrá detectar al llegar de nuevo a la entidad financiera. Esta dificultad se supera con la característica de trazabilidad, como es posible "seguir la pista" de quién ha realizado un determinado pago, cuando se detecte un uso fraudulento de las monedas electrónicas, se podrá penalizar a posteriori.

Además, la acción de pago difiere de la acción de depósito de fondos. Por ejemplo, Bob contactará con el Banco sólo una vez al día para ingresar todos los tokens recibidos en ese día.

La serie de mensajes enviados en dicho sistema es la que se describe a continuación.

Retiro de fondos

- Alice envía al Banco una solicitud de retiro de fondos.
- El Banco prepara una moneda electrónica y la firma digitalmente.
- El Banco envía la moneda a Alice y la carga en su cuenta.

Pago

- Alice entrega la moneda a Bob
- Bob verifica la firma digital del Banco (opcional)
- Bob da a Alice la Mercancía

Depósito de fondos

- Bob envía la moneda al banco
- El Banco verifica su firma digital.
- El Banco verifica que la moneda no ha sido ya gastada
- El Banco consulta su registro de retiro de fondos para confirmar el retiro por parte de Alice (opcional)
- El Banco introduce la moneda en la base de datos de la moneda gastada
- El Banco ingresa el dinero en la cuenta de Bob

Los dos protocolos anteriores usan firmas digitales para conseguir autenticidad. La autenticidad se puede conseguir por otros métodos pero se necesita el uso de firmas digitales para añadir los mecanismos que proporcionaran anonimato.

3.2 Pagos electrónicos no trazables.

En este apartado se describen las modificaciones que se realizan sobre los protocolos básicos ya presentados con el fin de impedir que los pagos sean trazables. Para esto es necesario que el banco no sea capaz de relacionar un determinado retiro de fondos con un ingreso en cuenta concreto. Habitualmente esta característica se consigue mediante el uso de un determinado tipo de firmas denominadas firmas ciegas o *blind signatures*.

En las firmas convencionales, el firmante conoce el contenido del documento digital que firma - tanto si lo ha generado él como si no - y lo cifra con su clave privada. En las firmas ciegas, sin embargo, el firmante no llega a conocer el contenido del mensaje que cifra ni lo genera él, por lo tanto se necesitan como mínimo 2 participantes para generar un documento firmado ciegamente, supongámoslos Alice y el Banco.

La encargada de generar el documento a firmar será Alice, ésta, antes de enviar el documento digital que el Banco debe firmar, modifica el mensaje que envía al Banco mediante el uso de un número aleatorio. Este paso se denomina "cegar el mensaje'" y al número aleatorio *blinding factor* o factor de cegado. Después del proceso de cegado el banco firma el mensaje aparentemente aleatorio y se lo devuelve a Alice. Finalmente Alice, que es capaz de "deshacer" el cegado, lo recupera.

A partir de este momento Alice posee un mensaje válido (que en nuestro caso puede ser una moneda electrónica) firmado por el Banco sin que éste se haya percatado de su contenido. El Banco será capaz de leer el contenido del mensaje cuando se le retorne en el proceso de depósito de fondos - téngase en cuenta que a partir del momento en que se retira el factor de cegado el mensaje viaja "en claro'" y firmado - pero no podrá asociar dicho mensaje al usuario que se lo ha hecho firmar, Alice, en nuestro caso.

Nótese que en el primero de los pasos a seguir el Banco no sabe qué es lo que está firmando, este hecho introduce la posibilidad que el Banco firme una cantidad distinta a la que Alice le "dice'' que está firmando. Para subsanar este problema el banco podría disponer de distintas "claves de firma'', de forma que, por ejemplo, use la clave K1 para firmar los mensajes supuestamente de importes no superiores a 10 euros, K2 para los mensajes entre 10 y 50 euros etc...

3.2.1 Pago electrónico on-line no trazable.

En los sistemas de pago no trazables la moneda la emite (o acuña) el comprador, y el Banco sólo se encarga de firmarla. Como la entidad financiera no es consciente de los "números de serie" de los billetes que están en circulación, ya que sólo los podrá ver cuando se le hayan devuelto, y por tanto, ya se hayan gastado, es crucial la prevención del doble uso. La solución es trivial en el sistema on-line (ya que la comprobación es en tiempo real) pero es de vital importancia en los sistemas off-line. De cualquier modo, para poder detectar quien es el defraudador, Alice debe identificarse frente a Bob, haciendo el sistema no trazable, pero tampoco anónimo.

La secuencia de mensajes intercambiados en el sistema on-line no trazable es la que se describe a continuación.

Retiro de fondos

- Alice crea una moneda electrónica y la ciega.

- Alice envía la moneda cegada al Banco con una petición de retiro de fondos de su cuenta.
- El Banco la firma digitalmente.
- El Banco devuelve a Alice la moneda firmada y la carga en su cuenta.
- Alice quita el factor de cegado de la moneda.

Pago/depósito de fondos

- Alice envía a Bob la moneda.
- Bob contacta con el Banco y envía la moneda.
- El Banco verifica la firma digital de la moneda.
- El Banco comprueba que la moneda no se haya utilizado con anterioridad.
- El Banco introduce la moneda en la base de datos de monedas gastadas.
- El Banco ingresa la cantidad en la cuenta de Bob y le informa.
- Bob entrega a Alice la mercancía comprada.

3.2.2 Pago electrónico off-line no trazable

El método de pago off-line no trazable es equivalente al on-line con la salvedad de la distinción de los procesos de pago e ingreso en cuenta. Como ya se comentó, para prevenir el doble uso, el comprador debe identificarse frente al vendedor. Así, aunque el Banco no puede trazar las compras, si el comprador realiza un doble uso, éste puede ser denunciado por el vendedor.

La secuencia de mensajes intercambiados son los que se describen a continuación.

Retiro de fondos

- Alice crea una moneda electrónica y la ciega
- Alice envía la moneda cegada al Banco junto con la petición de retiro de fondos.
- El Banco firma digitalmente la moneda cegada.
- El Banco devuelve la moneda cegada a Alice y la carga en su cuenta.
- Alice retira el factor de cegado de la moneda

Pago

- Alice entrega a Bob la moneda.
- Bob verifica la firma digital del Banco (opcional).
- Bob entrega a Alice la mercancía.

Depósito de fondos.

- Bob envía la moneda al Banco.
- El Banco comprueba su firma digital.
- El Banco comprueba que la moneda no haya sido ya gastada.
- El Banco introduce la moneda en la base de datos de monedas gastadas.
- El Banco ingresa la cantidad en la cuenta de Bob.

3.3 Protocolo de pago electrónico anónimo.

Finalmente, se le añadirán las modificaciones oportunas a los protocolos anteriores para garantizar anonimato en el pago. La condición ideal, desde el punto de vista de anonimato, sería que ni el Banco ni el Vendedor (Bob) conocieran la identidad del Comprador (Alice). Esto haría las transacciones electrónicas totalmente anónimas: nadie sabe donde Alice ha gastado su dinero y quién le ha dado ese dinero.

De cualquier modo, los protocolos usados hasta el momento sólo garantizan anonimato de comprador, es decir, el Banco sabe que Alice ha retirado dinero de su cuenta pero no sabe donde lo ha gastado y Bob sabe que el dinero proviene de un Banco en concreto pero no sabe quien es el comprador. Así decimos que se produce anonimato dos a dos. Si los pagos se realizan on-line el protocolo on-line no trazable ya garantiza dicha propiedad.

En el mecanismo off-line no trazable, sin embargo, como no deseamos que Alice desvele su identidad frente al Vendedor, aparecen nuevas dificultades. Si Bob quiere ingresar en su cuenta una moneda que ha sido gastada previamente no podrá, ya que el banco se lo impedirá, y además, nunca podrá saber quien ha gastado múltiples veces esa moneda, ya que se pretende que sea anónima.

Se ve la necesidad de un mecanismo mediante el cual el banco sea capaz de identificar un uso múltiple de una moneda y que a su vez garantice el anonimato de los usuarios de la moneda "legal" (no usada más de una vez).

En el momento en que se realice el pago, Alice deberá revelar cierta información a Bob, de esta forma se asegura que sólo Alice puede haber gastado la moneda ya que sólo ella conoce esa información.

Este procedimiento se realiza mediante lo que se denomina un protocolo de respuesta a desafío. En este tipo de protocolos, Bob envía a Alice un mensaje de desafío y Alice, como respuesta, le envía cierta información de identificación.

En el momento del depósito de fondos, Bob envía al Banco tanto la moneda como la respuesta al desafío. Si todos los participantes han actuado de buena fe, la información de identificación de Alice nunca desvelará su identidad. Si Alice, en cambio, decide gastar la moneda dos veces, deberá responder a dos desafíos (en principio) distintos. Cuando las dos monedas con los dos desafíos regresen al Banco la unión de las respuestas a los dos desafíos revelará la identidad de Alice. Mediante este procedimiento sólo los que deciden gastar la moneda dos veces serán identificados ya que el conocimiento de una única respuesta a un desafío no desvela ninguna identidad.

3.3.1 Pago electrónico no trazable anónimo.

Con todo lo expuesto anteriormente, el mecanismo de pago electrónico no trazable y anónimo queda descrito a continuación.

Retiro de fondos

-Alice crea una moneda electrónica que incluye información de identificación.
-Alice ciega la moneda.
-Alice envía la moneda cegada al banco con la petición de retiro de fondos.
-El Banco verifica que la información de identificación esté presente.

-El Banco firma la moneda cegada.
-El Banco devuelve la moneda firmada a Alice y la carga en su cuenta.
-Alice retira el factor de cegado de la moneda.

Pago

-Alice envía la moneda a Bob.
-Bob comprueba la firma digital del banco.
-Bob envía a Alice el desafío.
-Alice envía a Bob la respuesta (le revela una parte de su información de identificación).
-Bob comprueba la respuesta.
-Bob entrega a Alice el producto comprado.

Depósito

-Bob envía la moneda, el desafío y la respuesta al banco.
-El Banco verifica su firma digital.
-El Banco verifica que la moneda no se haya gastado previamente.
-El Banco guarda la moneda, el desafío y la respuesta en la base de datos de monedas gastadas.
-El Banco ingresa la cantidad en la cuenta de Bob.

Téngase en cuenta que en este procedimiento Bob puede comprobar la firma digital del banco antes de entregarle la mercancía a Alice, de esta forma Bob puede asegurar que o le ingresarán la cantidad en su cuenta o podrá saber quien ha gastado dos veces la misma moneda.

3.4 Características adicionales de los pagos electrónicos.

3.4.1 Transferibilidad.

La transferibilidad es una característica inherente en el papel moneda y que permite a su usuario gastar una moneda que acaba de recibir de otro usuario sin necesidad de contactar con el banco. Una transferencia, por tanto, será un pago en que el receptor puede usar la moneda en un pago posterior sin haber contactado con el Banco. Un sistema de pago es transferible si admite como mínimo una transferencia por moneda. En la figura 2 se puede ver el recorrido máximo de una moneda que permite dos transferencias.

La transferibilidad es una característica deseable en sistemas off-line porque requerirá menos conexiones con el banco. Un sistema de pago electrónico transferible es off-line por definición ya que los pagos on-line requieren conexión con el banco durante la transacción o transmisión del token.

Los sistemas transferibles no han recibido mucha atención por parte de la literatura académica. Cualquier sistema de pago electrónico transferible tiene el inconveniente que la moneda electrónica deberá "crecer de tamaño" cada vez que se gaste. Esto se debe a que la moneda debe añadir información de cada uno de los participantes en las distintas transferencias de forma que el banco pueda identificarlas en caso en que se produzca un uso doble de

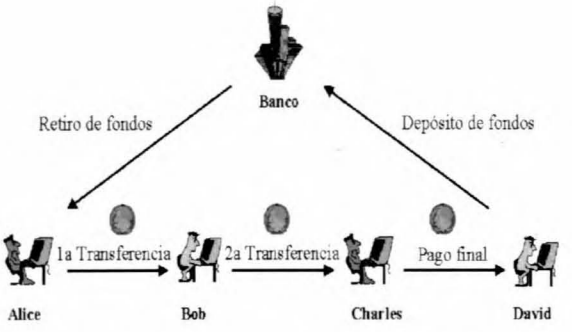

Figura 2. Esquema de pago transferible.

la misma. Este incremento de tamaño hace inviable un sistema de transferencias de número indeterminado y limita el máximo de transferencias permitidas a la capacidad de los sistemas informáticos que realizan la transacción.

Existen otros aspectos por los cuales los sistemas transferibles no han tenido demasiado éxito, incluso limitando el número de transacciones y no garantizando anonimato de los participantes. Hasta que la moneda no vuelve a ser depositada en el Banco, la entidad financiera sólo posee la información de quién ha realizado el retiro de fondos. Cualquier otra transacción sólo revelará la identidad de los participantes con la colaboración de éstos. Esto presenta el mismo problema que el papel moneda y su dificultad para detectar operaciones de blanqueo de dinero o evasión de impuestos: no existen registros de las transferencias realizadas.

Además, cada transferencia retrasa la detección de dobles usos o falsificaciones. Los usos múltiples de una moneda electrónica no se descubrirían hasta que como mínimo dos copias de la misma moneda se depositen en el banco. Por entonces, puede que sea demasiado tarde para detener al infractor y posiblemente muchos usuarios habrán recibido monedas electrónicas falsas. Esto pone de manifiesto que no es suficiente la detección del delito para sistemas de pago electrónico transferibles, sino que serán necesarios mecanismos de prevención del delito o a priori.

3.4.2 Divisibilidad.

Supongamos que Alice es una de las participantes de un pago electrónico no transferible y off-line, y quiere comprar a Bob un producto por valor de 4.5 euros. Si por casualidad tiene un conjunto de monedas electrónicas que juntas reúnen exactamente dicho valor no se presenta ningún problema, simplemente las entrega a Bob. De cualquier modo, a menos que Alice tenga una gran cantidad de monedas electrónicas y de distinto valor, es bastante improbable que reúna la cantidad exacta de "cualquier" compra.

Una posible opción sería que Alice retire del banco una cantidad exacta cada vez que quiera realizar una

compra, pero eso requiere interacción con el banco, convirtiendo al pago en on-line desde el punto de vista de Alice. La tercera opción sería que Bob "pagase" a Alice la diferencia entre lo que le ha entregado y el valor del producto, pero esta solución únicamente traslada al plano de Bob el hecho de disponer de monedas de una determinada cantidad y además requeriría que Alice contactase con el banco para "ingresar" el cambio.

Una solución a estos inconvenientes es el uso de monedas divisibles. Las monedas divisibles son monedas que pueden fragmentarse en partes cuyo valor total es igual al valor del original. Esto permitiría pagos off-line por una cantidad exacta sin la necesidad de acuñar monedas de distintas cantidades. Esta propiedad tal como aquí está planteada no la presenta el papel moneda, pero esta falta de divisibilidad se contraresta con su transferibilidad.

4. EJEMPLOS DE IMPLEMENTACIONES Y PROTOCOLOS REALES.

En este apartado se presentan los que se consideran los ejemplos más significativos de propuestas e implementaciones reales. La exposición se estructura según la clasificación de protocolos expuesta anteriormente. Para cada uno de los sistemas se detalla las empresas o instituciones que lo propusieron, las herramientas criptográficas en las que se basa, su modo de funcionamiento en cuanto a transacciones de mensajes se refiere y referencias donde encontrar más información.

Para entender los mecanismos aquí propuestos deberemos realizar una generalización del esquema básico de pago electrónico presentado en la figura 3.

En el nuevo esquema no se exige que comprador y vendedor tengan la misma entidad financiera, sino que ésta se desdobla en dos organismos: el Emisor de la moneda (o *Issuer* en inglés) y el Receptor del dinero (*Acquirer* en inglés). Así, el comprador retira su dinero del Emisor de moneda electrónica, efectúa un pago al vendedor quien a su vez deposita la moneda al Receptor. El flujo "real" de dinero se realiza entre *issuer y acquirer*.

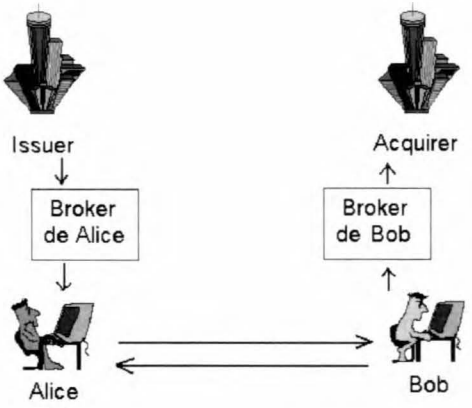

Figura 3. *Esquema general de pago electrónico.*

Adicionalmente puede aparecer la figura del *broker* o agente que, no siendo propiamente una entidad financiera, actuará como intermediario entre el Comprador o Vendedor y sus respectivos Bancos.

4.1 Sistemas on-line trazables.

Como ya se comentó cuando se expuso el procedimiento general de los sistemas trazables on-line, éstos son los de más fácil implementación; ésta es la razón por la que el número de implementaciones propuestas ha sido elevado. Aunque ya en desuso, se presentan First-Virtual, Cyber-Cash e iKP como ejemplos de propuestas anteriores al estándar SET. Este último, aunque con ciertas dificultades frente a sistemas de pago con tarjeta mediante SSL, pretende establecerse como estándar mundial de pagos on-line y trazables basados en tarjetas de crédito.

El problema más patente de los sistemas on-line es su elevado coste económico para la realización de pagos pequeños. La última parte de esta sección la dedicamos a exponer tres sistemas de micropagos on-line: NetBill, Millicent y MiniPay que pretenden subsanar dicho problema.

4.1.1 First - Virtual

Aunque ya totalmente en desuso, se presenta el sistema First-Virtual como uno de los primeros intentos de acomodar la infraestructura de comunicaciones existente a los protocolos de pago electrónico.

First Virtual Holdings Inc. propuso un sistema de pago que aprovechaba el correo electrónico para intercambiar mensajes entre el Vendedor y First-Virtual y el Comprador y First-Virtual. Esto eliminaba la necesidad de software y protocolos específicos y permitía a la empresa First-Virtual desarrollar su sistema a través de la infraestructura de Internet existente.

El sistema ofrecía anonimato del comprador frente al vendedor, pero la empresa First-Virtual, que actuaba como Broker, disponía de todos los datos, tanto del comprador como del vendedor. Uno de los aspectos que se presentaba como ventajoso era el hecho que ningún dato bancario "real" viajaba a través de la red, de esta forma se protegía frente a escuchas de terceros. Por el contrario, esto requería la existencia de un Identificador Virtual o y era necesario que tanto comprador como vendedor se diesen de alta (o hayan abierto una cuenta) en el Broker.

El protocolo seguía los siguientes pasos, véase figura 4:

(1) Alice inicia el proceso de compra de la forma habitual, pero en vez de enviar sus datos bancarios al vendedor, le envía su *Virtual-PIN*.
(2) Bob envía un correo a First Virtual (el *broker*) con la información del PIN de Alice,

el suyo propio, y una descripción de la compra.
(3) El Broker envía un correo a Alice con la información que le ha mandado Bob solicitando su confirmación.
(4) Alice envía por correo electrónico la confirmación al Broker.
(5) El Broker usa las redes financieras existentes para procesar la transacción mediante tarjetas de crédito (que dispone gracias a la base de datos, ya que tanto Alice como Bob están dados de alta en su servicio).
(6) En cuanto se ha realizado la transacción, el Broker envía un identificador de autorización a Bob.

Se puede encontrar más información sobre First Virtual en [Sir97].

4.1.2 CyberCash.

El sistema propuesto por CyberCash Inc. es muy similar al ya expuesto First Virtual en cuanto los dos utilizan las redes financieras existentes para realizar las transacciones reales de fondos y actúan a través de intermediarios o brokers.

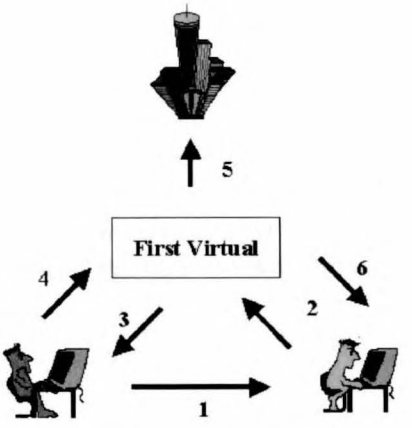

Figura 4. *Transacciones de datos implicadas en el sistema First-Virtual.*

El sistema básico CyberCash no es más que una pasarela que une a los vendedores en Internet con los sistemas de pago electrónico por tarjeta de crédito existentes. CyberCash simplemente integra el software del vendedor en las redes financieras existentes como si fuera un TPV (terminal punto de venta) más.

El sistema sigue los pasos descritos a continuación, véase figura 5:

(1) Alice realiza una orden de compra a Bob.
(2) Bob le contesta con una petición de pago.
(3) Alice genera un "pago cifrado" mediante el monedero CyberCash y se lo envía a Bob.
(4) Bob recorta el "pago cifrado" del mensaje que le ha enviado Alice, lo firma digitalmente y lo reenvía al servidor CyberCash.
(5) El servidor CyberCash traspasa la transacción de Internet a la red financiera, usa hardware específico para descifrarlo, formatea el mensaje de pago adecuadamente a la red financiera y lo envía al Banco de Bob.
(6) El Banco de Bob transfiere el mensaje de pago al Banco de Alice.
(7) El Banco de Alice confirma o deniega el pago y envía el resultado al Banco de Bob.
(8) El Banco de Bob envía el código de aprovación o denegación al servidor CyberCash.
(9) El Servidor CyberCash envía la aprobación o denegación a Bob.

Los 4 primeros pasos y el último se realizan a través de redes abiertas (Internet) mediante la combinación de criptografía de clave pública y simétrica. Los pasos 5,6,7 y 8 utilizan las redes financieras existentes. CyberCash estima que se puede realizar la transacción completa en un tiempo de 20 segundos aproximadamente. El sistema es atractivo para los bancos ya que sólo interactúan con ellos a través de sus redes financieras ya existentes.

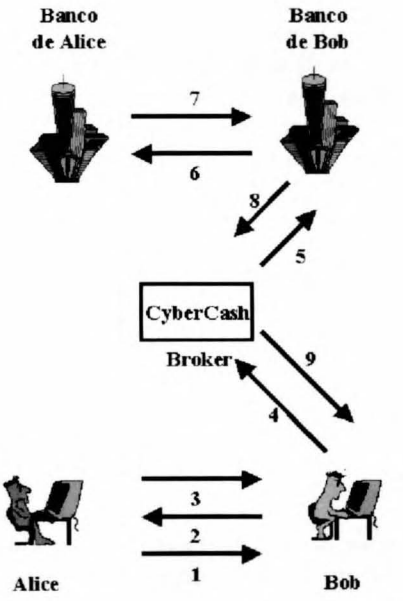

Figura 5. *Transacciones de datos implicadas en el sistema Cyber-Cash*

Cybercash también ha desarrollado mejoras de este sistema denominados CyberCoin, que consiste en un sistema on-line y trazable pero que soporta pagos pequeños (25 céntimos como mínimo) y CyberCheque. Todos estos sistemas son no anónimos y trazables. Puede encontrarse más información sobre CyberCash en [HREF1]

4.1.3 iKP

iKP o Internet Keyed Payment Protocols es una família de protocolos desarrollado por IBM Research Group. Todos los protocolos de la família se basan en criptografía de clave pública pero se diferencian en el número de participantes que se autentifican en el procedimiento de pago, este número es el indicado en el índice i:

• 1KP Sólo el Broker tiene clave pública y certificado.
• 2KP El Broker y el Vendedor disponen de herramientas de autenticación.
• 3KP Todos los participantes tienen certificado y clave.

El procedimiento de pago es análogo al de CyberCash, véase figura 5, aunque el formato de los mensajes implicados en la transacción es diferente. Al igual que en CyberCash, también existe una variante de este protocolo para la realización de micropagos denominado m-KP.

MasterCard, IBM, Netscape y CyberCash desarrollaron conjuntamente un sistema práctico de este protocolo, denominado Secure Electronic Payments Protocol (SEPP) considerado uno de los predecesores del SET. Puede encontrarse más información sobre iKP en [HREF2].

4.1.4 SET

SET o Secure Electronic Transactions es un estándar de pago seguro mediante tarjeta de crédito a través de Internet. Fue propuesto por MasterCard y Visa y auspiciado por la mayoría de entidades financieras y fabricantes de tecnología. Este sistema se basa en propuestas muy similares, entre las cuales están iKP de IBM, STT propuesto por Visa y Microsoft y SEPP desarrollado entre otros por MasterCard, IBM y Netscape.

Al ser un sistema basado en iKP y CyberCash, el diagrama de mensajes implicados en la transacción es muy parecido al de éstos aunque difiere en que, al pretender ser un estándar, no es necesaria la intervención de un broker sino que el mismo Banco del vendedor es quien ejerce esas funciones. Los pasos más detallados del sistema SET son los que se describen a continuación, véase figura 6.

(1) Alice realiza la orden de compra.

(2) Bob, el vendedor, envía al monedero de Alice, la compradora, la clave pública de su Banco, certificada por VISA/MC.

(3) Alice usa la clave pública de Bob para cifrar el número de su tarjeta de crédito. Emite la orden de pago firmada por ella misma, y la envía a Bob.

(4) Bob reenvía la orden de pago a su Banco.

(5) El Banco de Bob usa la red financiera existente para cursar la orden de pago hasta el Banco de Alice. Este procedimiento sólo se diferencia de una transacción por tarjeta de crédito convencional en que se indica que se trata de una operación SET.

(6) El Banco de Alice confirma el pago al Banco de Bob.

(7) El Banco de Bob envía un recibo de pago firmado a Bob.

(8) Bob envía el recibo firmado a Alice.

Aunque actualmente es el sistema de pago estándar, se deben hacer algunas consideraciones sobre el sistema SET. Debido a que la clave pública del banco de Bob debe estar firmada por VISA/MC, sólo los bancos autorizados por dichas firmas comerciales podrán integrarse dentro del sistema SET. En segundo lugar, cuando los mensajes de transacción se introducen dentro de la red financiera existente pierden la firma del comprador, es decir, la orden de pago no viaja firmada por el comprador, careciendo entonces de la propiedad de no repudio, aunque a nivel práctico existan suficientes pistas como para trazar el mensaje y garantizar cierto nivel de no repudio.

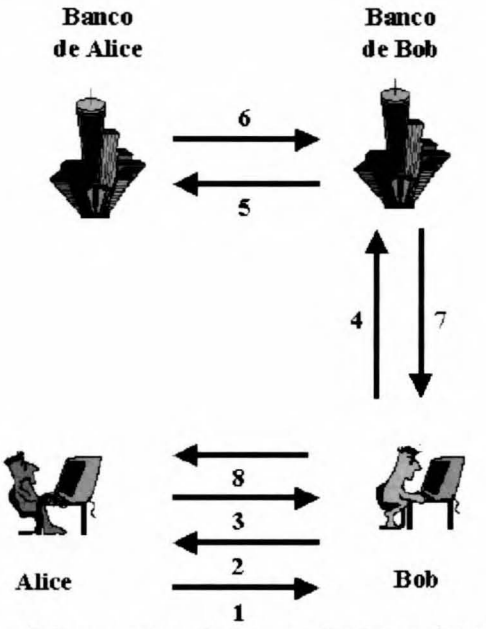

Figura 6. Transacciones de datos implicadas en el sistema SET

Finalmente, apuntar que el sistema SET entra en competencia con los sistemas de pagos mediante tarjetas de crédito tradicionales con transmisión segura de datos bancarios sobre el protocolo SSL, que es hoy en día el mecanismo más extendido, aunque no se trate de un protocolo de pago propiamente dicho.

Puede hallarse información más detallada sobre el sistemas SET en [HREF3].

Sistemas on-line trazables para micropagos.

Los pagos con tarjeta de crédito tienen un coste muy elevado en cuanto a comisiones por servicio se refiere, alrededor de un 2% con tasas mínimas del orden de 25 céntimos de euro. Además, el proceso de autorización implica retardos considerables en el tiempo de compra. Estos dos problemas son los más significativos a la hora de realizar pagos de pequeñas cantidades.

4.1.5 NetBill.

La Universidad de Carneggie Mellon junto con la empresa CyberCash desarrollaron en 1997 un sistema de pago basado en cheques electrónicos denominado NetBill.

Dicho sistema usa tanto criptografía de clave pública como simétrica para garantizar los servicios de seguridad requeridos. Al igual que el sistema de pagos y macropagos First Virtual, NetBill requiere que tanto vendedor como comprador dispongan de una cuenta abierta en una central (o broker) de NetBill. El sistema está pensado para la venta de productos electrónicos (música, vídeo a través de internet, documentos...)

El mecanismo de funcionamiento consta de 6 pasos y se describe a continuación, véase figura 7:

(1) Alice realiza una petición de compra "pay-per-click".

(2) Bob envía a Alice el producto electrónico cifrado junto con una función resumen del producto cifrado.

(3) Alice, mediante el hash, comprueba que el producto cifrado se ha recibido de forma correcta y devuelve un mensaje de verificación a Bob.

(4) Bob envía el mensaje de verificación, la información de la cuenta NetBill de Alice y la clave de descifrado del producto comprado al servidor NetBill.

(5) NetBill comprueba la existencia de fondos en la cuenta de Alice, realiza la transferencia entre cuentas y lo notifica a Bob.

(6) Bob envía la clave de descifrado del producto a Alice. Si Bob no envía la clave de descifrado, Alice puede pedirsela al servidor NetBill directamente.

Se puede obtener más información sobre este sistema de micropago en [HREF4].

4.1.6 Millicent.

Millicent es un "Sistema de Microcomercio Digital" propietario, desarrollado por la empresa Digital Inc. Se basa en el uso de bonos o *scrips*, que consisten en un determinado tipo de tokens que sólo son válidos para un vendedor en particular y un broker concreto. Este hecho elimina la necesidad de conectarse a un determinado emisor o *issuer* para comprobar la validez de los tokens reduciendo por tanto el tráfico ofrecido a la red.

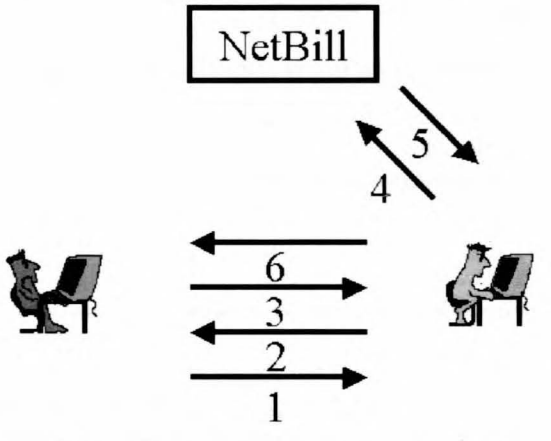

Figura 7 *Esquema de transacciones en el sistema NetBill.*

El sistema se descompone en los siguientes pasos, figura 8:

(1) Alice obtiene una determinada cantidad de bonos del broker.

(2) Alice solicita bonos de un determinado vendedor a su broker.

(3) El Broker obtiene los bonos de Bob.

(4) El Broker vende los bonos de Bob a Alice.

(5) Alice compra los productos de Bob pagándole con sus bonos.

(6) Bob le devuelve el cambio a Alice mediante bonos de Bob.

Se puede obtener más información sobre este sistema de micropagos en [HREF5].

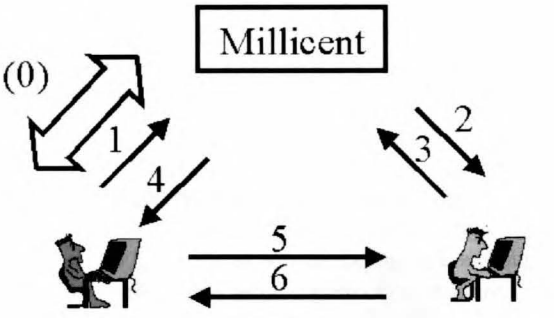

Figura 8. *Transacción según Millicent*

4.1.7 MiniPay.

MiniPay es un mecanismo de pago desarrollado por IBM que pretende superar los problemas presentados por sistemas anteriores para la realización de micropagos: ofrece bajo coste (menos de un céntimo de euro por transacción) y retardo despreciable.

Los mecanismos de seguridad que utiliza son firmas digitales, certificados y hashes. MiniPay minimiza el tráfico ofrecido a la red ya que la validación de los tokens se realiza semi on-line, es decir, sólo se contacta con la entidad emisora o receptora una vez al día o en caso de detectarse un gasto superior a cierto valor.

La idea básica es que issuer y acquirer son los respectivos Proveedores de Acceso o Servicios de Internet de Alice y Bob, así que están on-line si sus respectivos clientes entán on-line. Cada comprador obtiene un "límite de gasto" autentificado de su respectivo Proveesor de acceso. Cada comprador acepta compromisos de pago de los usuarios autentificados de manera off-line, y sólo realiza la comprobación on-line si la cantidad comprometida supera un determinado valor.

El esquema en sí consta sólo de 3 pasos, aunque una vez al día se produzcan las transacciones periódicas correspondientes, o eventualmente se realicen comprobaciones on-line, véase figura 9.

Puede encontrarse más información de este sistema en [HREF6]

Otros sistemas de micropagos.

Existen otros sistemas de micropagos, se ha presentado un ejemplo de sistema de micropagos basado en cadenas de hash invertidas, otro basado en bonos y finalmente otro basado en tarjetas de débito. Además de éstos también existen variaciones de los mismos denominados Netcard [HREF7], Payword [HREF8], Agora [HREF9] entre otros...

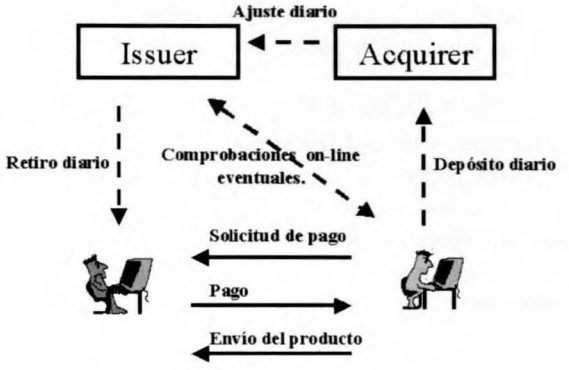

Figura 9. *Transacciones en MiniPay.*

4.2 Sistemas off-line trazable.

Un paso más hacia las características que apuntábamos que debía tener la moneda electrónica era su condición de off-line, evitar la comprobación de la validez del token durante el proceso de transacción. Recordemos que el mayor peligro que presentaban este tipo de sistemas era la amenaza de *double spending*.

En esta sección presentamos dos propuestas de sistemas prácticos off-line aunque trazables. El primero se protege frente al doble uso mediante el uso de tarjetas inteligentes o smartcards. Es decir, evita la duplicación del token basándose en la dificultad de duplicar un dispositivo hardware; en última instancia, este es el mismo método que se utiliza en el papel moneda tradicional en los que la falsificación de papel moneda, aunque no imposible con suficientes medios, es técnicamente muy costosa. Este tipo de tarjetas se denomina en la literatura *tamper proof devices* o dispositivos a prueba de copia.

El segundo de los sistemas que se presenta se basa en la emisión de cheques electrónicos, mecanismo análogo a los cheques tradicionales, en este sistema no se puede evitar que un usuario "emita" el mismo cheque varias veces o que éstos no tengan fondos, pero como se trata de un sistema trazable, el delito es detectable y punible.

En los sistemas off-line, retiro de fondos, pago y depósito se realizan en instantes temporalmente diferenciados. El pago sólo implica a Alice y Bob, y normalmente sólo consta de 3 pasos: solicitud de compra, solicitud de pago y envío de token. En este tipo de sistemas no tiene tanta importancia la secuencia de mensajes generados como las técnicas empleadas y su robustez.

4.2.1 Mondex.

Mondex es un sistema propuesto por MasterCard en 1995. Proporciona un sistema de pago mediante el uso de tarjetas inteligentes. Es un sistema propietario del cual se conocen muy pocas especificaciones técnicas. Concebido principalmente para la realización de micropagos, existe una versión que adapta el sistema para realizar pagos a través de Internet, aunque es necesario el uso de lectores de tarjetas en los PC's involucrados.

La ventaja de Mondex es que no necesita verificación on-line generando mucho menos tráfico que en las transacciones off-line. En cambio, el sistema no proporciona anonimato y el banco puede trazar todas las transacciones y construir perfiles de usuario.

Puede encontrarse más información sobre Mondex en [HREF10].

4.2.2 FSTC Electronic Check Project

FSTC o Financial Services Technology Consortium propuso en 1997 un sistema off-line trazable basado en la idea de cheques electrónicos. La propuesta forma parte del proyecto BIPS, que se centra en el estudio de un modelo general de integración de las infraestructuras financieras existentes en los pagos a través de Internet.

En los cheques convencionales la entidad financiera da "permiso" al usuario para que "emita" un documento similar al papel moneda, para que a posteriori se lo cargue en su cuenta y lo abone al "portador" de ese cheque. Como el cheque está identificado, el fraude se puede detectar y penar. El sistema FSTC sigue la misma idea pero de forma electrónica.

Alice firma digitalmente el cheque para garantizar autenticación y Bob, a su vez, también lo firma para garantizar no repudio. Es necesaria la existencia de certificados de comprador, vendedor y cuenta bancaria para realizarse la transacción. El Cheque, una vez emitido, puede enviarse por cualquier medio existente, e-mail, por ejemplo.

Aunque en principio no son necesarias las tarjetas inteligentes o cualquier otro dispositivo hardware, se recomienda el uso de éstas para generar las firmas de los participantes en la transacción sin comprometer la privacidad de su clave secreta. Puede encontrarse más información sobre FSTC en [HREF11].

Otros Sistemas Off-line trazables.

En [Com97] se apunta la existencia de otras propuestas de sistemas off-line trazables, la mayoría basados en dispositivos tamperproof del tipo tarjetas monederos, denominados CLIP, CEN Intersector Electronic Purse, EMV Electronic Purse, aunque las referencias a hipertexto allí indicadas ya no estaban disponibles.

4.3 Sistemas on-line no trazables.

Otro paso intermedio hacia los sistemas de moneda electrónica son los sistemas on-line no trazables, en ellos la comprobación del token se realiza justo en el momento de la transacción pero la confabulación de Vendedor y Banco no desvela el rastro de las compras de Alice.

Es difícil conseguir un anonimato total, más incluso en sistemas on-line, donde como mínimo se revela la conexión que se realiza (IP del host de emisión y recepción por ejemplo). La mayoría de sistemas que dicen que ofrecen esta garantía lo hacen desplazando la responsabilidad de unir datos bancarios (o dinero) y producto comprado a un tercer agente, supuestamente de confianza, que aunque capaz de trazar todas las compras, se compromete a no desvelar dichos datos.

4.3.1 NetCash.

NetCash es un sistema propuesto en 1996 por G. Medvinsky y B.C. Neuman del *Information Sciences Institute* de la Universidad de California del Sur. Está orientado a micropagos.

Ofrece un sistema de pago seguro y anónimo en tiempo real. Como técnicas criptográficas utiliza certificados, firmas digitales y control de doble uso mediante base de datos. No necesita hardware especial ni redes seguras, y está especialmente pensado para su uso en Internet.

El sistema de detección de doble uso o doble gasto implementado en NetCash es inverso al empleado normalmente por las otras propuestas. NetCash guarda una base de datos con el número de serie de billetes emitidos y no de billetes gastados, como es habitual, y los borra de su base de datos cuando se han gastado. Se pretende así no tener que mantener indefinidamente una base de datos de billetes usados. La comprobación de la validez del token se realiza on-line.

La no trazabilidad ofrecida por NetCash es una no trazabilidad reducida ya que aunque el Banco no será capaz de seguir el rastro del comprador ni construir perfiles de usuario, ésta amenaza se traspasa al Servidor NetCash. Puede encontrarse más información sobre NetCash en [HREF12].

4.3.2 Anonymous Credit Cards (ACC).

ACC pretende ofrecer un sistema de tarjetas de crédito no asociado a una determinada persona física. Fue propuesto en 1994 por D. Kristol, S. Low, M. Maxemchunk y S. Paul de los Laboratorios AT&T Bell y está concebido para la realización de compras de bienes tangibles en centros comerciales de forma presencial.

La idea básica es separar la información necesaria para la transacción económica en distintas partes según sean datos requeridos por cada uno de los integrantes de la transacción. Una vez esté separada dicha información se usan técnicas criptográficas para ocultar a cada participante la información que no requiere.

Con el sistema ACC Alice se encuentra físicamente en el centro comercial donde realiza la compra y la realiza de forma presencial, en cambio, su identidad no le es revelada a Bob. El protocolo tiene una versión extendida para la realización de compras en internet denominada AIMP (*the Anonymous Internet Mercantile Protocol*). Puede encontrarse más información en [HREF13].

4.4 Sistemas off- line no trazables.

Los sistemas off-line no trazables son los de más difícil realización, y es por esto que son los que menos propuestas han recibido en la literatura. En ellos se unen todos los incovenientes de los sistemas off-line y todos los de los sistemas no trazables. Como solución a los problemas off-line se opta por el uso de tarjetas inteligentes y como solución a los problemas planteados por la no trazabilidad se optó por no asociar ninguna cuenta bancaria ni dato personal al dispositivo hardware, sino "depositar" el dinero en el mismo dispositivo, de forma que si se pierde o deteriora la tarjeta, se perderá o deteriorará el dinero real. Esta última característica es completamente análoga al papel moneda.

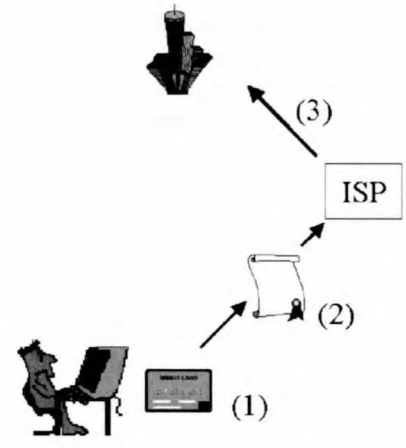

Figura 10. *Esquema del sistema off-line no trazable propuesto por S. Brands.*

4.4.1 Brands Cash.

Uno de los primeros sistemas off-line no trazables fue propuesto por Stefan Brands en [Bra93] y [Bra95]. El sistema se basa en dispositivos hardware para evitar el doble uso, en concreto en tarjetas PCMCIA y en criptografía de clave pública y firmas digitales para evitar repudio. Un esquema simplificado del mismo se puede ver en la figura 10.

En la tarjeta inteligente existe un contador que actualiza el saldo del usuario. El sistema se basa en criptografía de clave pública, existe una clave pública y otra secreta que sólo conoce la Smartcard. El PC actúa como interfaz entre la tarjeta e Internet (1). El sistema emite un cheque electrónico con la firma de la tarjeta (o de su propietario)sobre la cantidad expresada en el cheque y lo envía al Proveedor de Servicios de Internet (2), el cual transcribe el pago hasta el banco o la entidad financiera (3). Este sistema se considera el padre de CAFE.

4.4.2 CAFE

CAFE o Conditional Access For Europe fue propuesto por la Union Europea, la universidad de Leuven y un grupo de empresas entre las que se encuentran Digicash, CWI y Siemens. Es un sistema off-line de moneda electrónica con garantía de anonimato. Puede encontrarse más información sobre este sistema en [HREF14].

Otros sistemas

El mayor inconveniente de este tipo de sistemas es que necesitan de tarjetas inteligentes o smartcards para su implementación, y éstas presentan aun varios problemas. En [Cha99] se exponen los inconvenientes de la utilización de tarjetas inteligentes: falta de movilidad, ya que al depender de un lector de tarjetas, la movilidad también depende de éste, y además, al no existir un único estándar de lector, cualquier PC debería disponer de todos los posibles lectores para garantizar movilidad absoluta; elevado coste tanto del lector como de la tarjeta para el montante que habitualmente implicará dicho tipo de pagos; e ineficiencia de cálculo, ya que en algunas implementaciones de tarjetas inteligentes se han detectado tiempos de cómputo superiores a implementaciones basadas en software. Estos inconvenientes se presentan como los motivos principales por los cuales no ha tenido éxito dicha tecnología.

5. CONCLUSIONES

En este artículo se ha realizado una introducción a los sistemas de pagos electrónicos, su evolución, situación actual y retos futuros. En primer lugar se presentó la nomenclatura y definiciones básicas usadas en el campo del comercio electrónico para facilitar la comprensión de los siguientes apartados y dar una uniformidad de lenguaje al documento. Igualmente se expuso el conflicto existente a la hora de caracterizar los sistemas de pago electrónico, especialmente la dicotomía planteada entre sistemas autenticados o anónimos y trazables o repudiables. Asimismo, se planteó una posible vía de solución, se introdujo el concepto global de legitimidad y se trasladaron las características antes mencionadas a un plano más concreto dependiente del método de pago electrónico usado.

A continuación se presentaron los protocolos genéricos capaces de proporcionar cada una de las características mencionadas, se destacó la especial dificultad de proporcionar sistemas anónimos off-line y no trazables. Finalmente se expusieron los sistemas reales que implementaban los protocolos expuestos de forma genérica.

Del estudio de la evolución de los sistemas reales presentados se deduce que el éxito o el fracaso de un determinado esquema depende en gran medida del esfuerzo estandarizador y el apoyo de las grandes entidades financieras, que serán las principales "clientes" de dichos sistemas, así como de los estados, que son los responsables actuales de "emitir" el dinero en circulación, y que ven con cierto recelo la aparición de dinero "acuñable" por entidades no controladas por ellos.

De todos modos, ejemplos como el SET ponen de manifiesto que, a parte de la necesidad de estandarización y apoyos de entidades financieras, es preciso no perder de vista soluciones técnicas baratas, abiertas y compatibles con infraestructuras ya existentes, como el pago con numeración de tarjetas de crédito sobre HTTP seguro. En ese sentido Schneier apunta en [Sch99] la importancia que tiene en criptografía el hecho de "no ser diferentes".

Por otro lado, existen sistemas de pago menores basados en bonos, en cheques o en terceras partes (brokers) emisoras de moneda, que aunque no lleguen a escalas de universalidad comparables con los ya mencionados si pueden ofrecer soluciones a casos

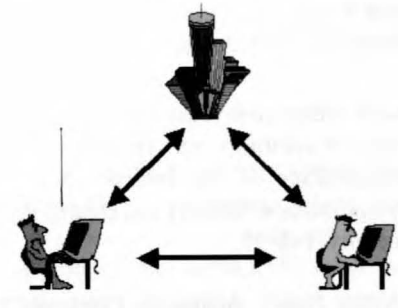

Figura 11. *Esquema circular de pago electrónico.*

concretos. Este tipo de sistemas, en cambio, presenta la dificultad de integración (necesidad de infraestructura y acuerdos) con las redes financieras existentes.

Otro punto que se ha puesto de manifiesto es la relación casi unívoca entre las características requeridas por un sistema con las herramientas criptográficas usadas para conseguir dichas características. Así, por ejemplo, el gasto doble en sistemas anónimos se evita principalmente mediante el uso de hardware tamperproof, y no se han encontrado estudios que presenten alternativas a dicha tecnología. Como el uso de tarjetas inteligentes presenta muchos inconvenientes, tal como expone Chadwick en [Cha99b], se prescinde de sistemas reales anónimos y así se aseguran la detección del infractor.

Si a lo expuesto anteriormente se le añade la precaución que suscita el anonimato en las transacciones electrónicas debido a la potencialidad de fraude y uso ilícito que de él se deriva, concluiremos que, aunque técnicamente viable, no existe voluntad de impulsar los sistemas de pago anónimos, y los pretendidamente existentes son fácilmente rastreables.

De igual forma, se observa que la totalidad de los sistemas expuestos depositan la responsabilidad en el vendedor. Es decir, el vendedor es quien toma la iniciativa en cuanto a transacción de mensajes válidos, y por tanto, el comprador adopta un papel pasivo y más indefenso frente a posible fraude por parte del vendedor.

En todos los esquemas presentados existe una estructura común cerrada, véase figura 11, que además de pasividad en el comprador, favorece la confabulación de Banco y Vendedor.

REFERENCIAS

[Bra93] Brands, S. An Efficient Off-line cash system based on the representation problem} Centrum voor Wiskunde en Informatica(CWI) Technical Report CS-R9323. March 93

[Bra95] Brands, S Electronic Cash on the Internet Centrum voor Wiskunde en Informatica (CWI) Proceedings of the Internet Society 1995 Symposium on Network and Distributed System Security. Feb 95.

[Cha92] Chaum, David. Achieving Electronic Privacy, Scientific American, August 1992, p. 96-101.

[Cha99] Chadwick D. Smart Cards Aren't Always the Smart Choice}, IEEE Computer. December 1999

[Leo98] Leong, Anthony. Paper, Plastic, and Now, Electronic: A survey of Electronic Payment Systems 1998.

[Oka92] Okamoto, T., Ohta k. Universal Electronic Cash. Advances in Cryptology, CRYPTO'91 Springer Verlag, 1992, pp324-337

[Sch99] Schneier B. Cryptography: the Importance of not Being Differet. IEEE Computer March 1999

[Sir97] Sirbu, Marvin. Credits and debits on the internet. IEEE Spectrum. Feb 97

[Com97] VV.AA The state of the art in electronic payment systems. IEEE Computer Sept 97.

REFERENCIAS A HIPERTEXTO

[HREF1] http://www.cybercash.com

[HREF2] http://www.zurich.ibm.com/Technology/Security/extern/ecommerce/iKP.html

[HREF3] http://www.dlib.org/dlib/january98/ibm/01herzberg.html

[HREF4] http://www.netbill.com

[HREF5] http://www.millicent.digital.com

[HREF6] http://www-4.ibm.com/software/webservers/commerce/payment/mpay/index.htm

[HREF7] http://www.cl.cam.ac.uk/~cm213/Project/project_publ.html

[HREF8] http://theory.lcs.mit.edu/~rivest/RivestShamir-mpay.ps

[HREF9] http://www.bell-labs.com/user/eran/agora.html

[HREF10] http://www.mondex.com

[HREF11] http://www.fstc.org

[HREF12] http://www.isi.edu/gost/info/netcash/

[HREF13] http://portal.research.bell-labs.com/lateinfo/projects/ecom.html

[HREF14] http://www.cwi.nl/cwi/projects/cafe.html