Sistemas de pago electrónico

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

PID_00199787

UOC
Universitat Oberta de Catalunya

Índice

Introducción

Con la aparición y generalización del comercio electrónico se ha hecho necesaria la creación de sistemas electrónicos de pago adaptados a la situación no presencial de los usuarios involucrados. Con los pagos electrónicos se pretende conseguir un medio de pago que presente un conjunto de características propio de los sistemas de pago físicos, a la vez que permita realizar transacciones sin que los usuarios se encuentren físicamente, es decir, que se permitan transacciones remotas.

Los sistemas de pago electrónico presentan mucha diversidad. Algunos de ellos se basan en la infraestructura de tarjetas bancarias existentes, mientras que otros intentan emular las prestaciones de la moneda física. En cualquiera de los casos se deberá garantizar la seguridad del sistema. Las medidas de seguridad criptográficas sustituyen (o complementan) las medidas de seguridad físicas, como los hologramas, los hilos de seguridad o las marcas de agua en la moneda física y las bandas magnéticas y los chips en las tarjetas de crédito o débito.

La moneda física es un medio de pago tradicional, que presenta como característica importante (a diferencia de otros sistemas de pago) la posibilidad de realización de pagos anónimos. Esta será una característica deseable a la hora de construir un nuevo medio de pago electrónico.

Otros medios de pago habituales en el mundo físico podrían ser utilizados en transacciones remotas. Las tarjetas bancarias son un ejemplo de ello. A diferencia de la moneda física, las tarjetas bancarias no son anónimas y permiten el monitoreo de las transacciones y la creación de perfiles de clientes, a causa de la posibilidad de enlace de los diferentes pagos realizados por el mismo usuario. También se deberá tener en cuenta que las medidas de seguridad basadas en la presencia física de la tarjeta (banda magnética, chip) no se utilizan en estas transacciones a no ser que se disponga de un lector de tarjetas. La seguridad basada en la presencia física se puede sustituir por el uso de técnicas de seguridad no presenciales. Si no es así, la utilización de manera autónoma del número de la tarjeta presenta problemas de autorización del pago.

1. Tipos de sistemas de pago electrónico

Entre los pagos electrónicos se pueden distinguir varias categorías. La clasificación se puede hacer en función de diferentes criterios, teniendo en cuenta el margen de cantidades de los pagos que se pueden realizar en el sistema, así como la semejanza y la utilización de elementos de medios de pago convencionales. La eficiencia y los costes asociados a las transacciones realizadas con las diferentes categorías condicionan la magnitud de los pagos que se pueden realizar con cada una de ellas. De este modo, unos costes asociados elevados implican un límite inferior en la magnitud de los pagos e imposibilitan pagos de pequeñas cantidades. Por otra parte, la reducción de medidas de seguridad permite reducir los costes y mejorar la eficiencia pero, como consecuencia, no permite realizar pagos de grandes cantidades de manera totalmente segura.

Una de las tres barreras existentes que limitan la extensión del comercio electrónico, junto con la facilidad de uso y el acceso al hardware requerido, es la falta de privacidad. Por este motivo, otro aspecto diferenciador en los sistemas de pago electrónico es el grado de privacidad que ofrecen. Nos encontramos con sistemas en los que los usuarios son totalmente identificados, con sistemas que permiten que el pagador se mantenga anónimo ante el receptor del pago, pero que exigen que se identifiquen frente al banco (y como consecuencia el banco es capaz de relacionar al pagador con un depósito del receptor del pago) y con sistemas totalmente anónimos, donde no se puede descubrir la relación entre un comprador y la compra realizada. Otra propiedad que se debe tener en cuenta es la posibilidad de uso anónimo del dinero recibido en un pago.

La presencia o ausencia de partes adicionales (diferentes del pagador y el receptor) durante el pago divide los sistemas en dos categorías: en línea y fuera de línea. Más adelante se verá que la ausencia de terceras partes durante la fase de pago se considera una característica deseable.

Finalmente, también se podría hacer una clasificación en función del momento en el que se hace la transferencia real del dinero. Con esta clasificación podríamos dividir los sistemas en: sistemas a crédito, sistemas de pago instantáneo y sistemas de prepago.

Una posible división de los sistemas de pago electrónico distingue cuatro grupos:

1) Cheques electrónicos. Los cheques electrónicos, sustitutos de los cheques de papel, proporcionan un mecanismo para realizar una transferencia de fondos entre la cuenta bancaria del pagador y la cuenta bancaria del receptor. Un cheque electrónico es un mensaje con una signatura digital, que representa un valor monetario, que se hace efectivo a través de una tercera parte. En este tipo de pagos se hace uso de las redes interbancarias existentes.

2) Moneda electrónica. Esta alternativa emula las características de la moneda física. El anonimato es su característica diferenciadora, ya que se pretende que la moneda electrónica permita realizar pagos que no queden registrados y no vinculen a los usuarios con sus compras. Otras características que se intentan conseguir son la transferencia fuera de línea, la transferibilidad y la seguridad frente a la falsificación o al uso de la moneda en más de un pago.

3) Tarjeta de crédito. En los pagos donde la tarjeta de crédito está presente se pueden realizar verificaciones en línea durante las transacciones. Por otra parte, la utilización de tarjetas de crédito sin la presencia física del pagador (y por tanto de su tarjeta), ya sea en pedidos telefónicos, por correo o en comercio electrónico, presenta el problema de la identificación del usuario, ya que no se puede realizar la verificación de la tarjeta ni de la firma manuscrita del usuario. En los sistemaes de pago electrónico mediante tarjeta de crédito, los receptores se pueden poner en contacto con el banco para verificar la disponibilidad de fondos, pero normalmente no se realiza la verificación de la identidad del usuario, sino que se permite el pago con la introducción del número de la tarjeta y su fecha de caducidad, únicamente. El protocolo SET se propuso como protocolo de pago que utiliza las tarjetas de crédito tradicionales como medio de pago sustituyendo las medidas de seguridad físicas por otras criptográficas (como la firma electrónica) que permiten la identificación del titular de la tarjeta. La autenticación del usuario también se puede realizar ante su entidad bancaria o ante la entidad emisora de la tarjeta utilizando diferentes técnicas (vía telefónica, introducción de pin, etc.). A diferencia de la moneda electrónica, que puede ser anónima, las tarjetas de crédito identifican a su propietario, y además los pagos se pueden vincular entre ellos.

4) Micropagos. Los micropagos se diseñan especialmente para reducir los costes de comunicación, almacenamiento y procesamiento relacionados con el pago. De esta manera, el límite inferior que permite un sistema de micropago se adapta a las compras más pequeñas. Estos pagos, al ser de pequeñas cantidades, permiten relajar las medidas de seguridad, ya que los riesgos están más controlados. En la mayoría de los sistemas de micropago el anonimato del usuario que realiza el pago se sacrifica para reducir costes.

2. Sistemas de pago mediante tarjeta de crédito

Los sistemas de pago actuales son muy parecidos a los sistemas que se utilizaban hace algunas décadas, cuando las transacciones se realizaban cara a cara. En el entorno del mundo real, el posible fraude asociado a estos tipos de pagos se puede mitigar mediante políticas de uso, mecanismos de seguridad físicos o control de infraestructuras. En las transacciones en las que la tarjeta no se presenta físicamente aparecen nuevas maneras de cometer fraude.

Para llevar a cabo un pago seguro y confiable utilizando tarjetas, se deben tener en cuenta una serie de propiedades:

- Validez de la tarjeta. Se debe comprobar que la tarjeta presentada es un medio de pago válido.
- Autenticación del propietario. El usuario que presenta la tarjeta para efectuar el pago ha de ser su legítimo propietario.
- Confidencialidad. Los detalles del pago utilizados en la transacción no deben estar a disposición de ninguna tercera parte.
- Privacidad. Los datos de pago y de la tarjeta, así como la relación entre la identidad del propietario y una compra, no debe ser utilizada por partes no autorizadas ni por propósitos diferentes a la propia compra.
- Efectividad. El coste asociado al uso del mecanismo de pago mediante tarjeta ha de permitir que el pago sea efectivo y viable.

En los pagos en el mundo real la autenticación de la tarjeta se realiza según características físicas de esta, como hologramas, bandas magnéticas, etc. La autenticación del propietario se realiza mediante la comprobación de la firma, de la fotografía o presentando un documento acreditativo.

Cuando los pagos se hacen en modo no presencial, la autenticación se debe realizar utilizando otros métodos, el más sencillo de los cuales es la presentación de datos adicionales al número de tarjeta, como puedan ser el código de seguridad, la fecha de caducidad o la dirección postal asociada a la tarjeta.

El protocolo SSL establece un canal de comunicación seguro entre dos ordenadores. Los usuarios podrán intercambiar datos de manera segura y opcionalmente autenticarse mutuamente. En las operaciones de comercio electrónico,

habitualmente el comerciante se autentica frente al consumidor, pero este último no está obligado a hacerlo. La utilización de SSL en las operaciones de pago mediante tarjeta de crédito permite que los datos asociados al pago, como el número de tarjeta, se transmitan de manera segura, obteniendo confidencialidad. No obstante, los pagos utilizando SSL aún sufren la falta de autenticación del propietario de la tarjeta. Tampoco permite controlar el uso que el comerciante hace de los datos de pago recibidos, lo que obliga al pagador a confiar en el comerciante. A pesar de estos problemas, SSL es ampliamente utilizado en los pagos actuales.

Solucionar el problema del conocimiento de los datos de pago por parte del comerciante es posible utilizando SET. SET es un protocolo que fue desarrollado por Visa y Mastercard para permitir transacciones electrónicas seguras. SET permite la autenticación de los dos actores del pago. Gracias a la utilización de firmas duales, SET permitía que solo la entidad de pago pudiera ver la información de pago asociada a la operación de compra, al mismo tiempo que solo el comerciante pudiera ver la orden de compra. Las características de SET y de la firma dual permiten que el comerciantes pueda confiar en la ejecución del pago pese a no conocer los datos de pago. A pesar de presentar una buena solución a los problemas de los pagos con tarjeta de crédito, SET fracasó. Probablemente el hecho de requerir la autenticación del comprador y la necesidad de este de adquirir un certificado digital fue determinante.

Firma dual

La firma dual vincula dos mensajes que se enviarán a dos destinatarios diferentes. Cada receptor recibirá una firma sobre la concatenación de los resúmenes de los dos mensajes, así como el mensaje que le corresponde. De esta manera, no podrá conocer los contenidos del segundo mensaje pero sí demostrar su vinculación.

Actualmente los sistemas de pago basados en el entorno de los tres dominios permiten mejorar la fase de autenticación del usuario respecto al uso de SSL, aunque sin la necesidad de certificados digitales y, por tanto, manteniendo la facilidad de uso. En el 3D Secure los usuarios deberán superar una fase de autenticación en el momento de utilizar la tarjeta de crédito en un establecimiento virtual. El mecanismo utilizado depende de la entidad bancaria y del emisor de la tarjeta. Se pueden encontrar mecanismos de autenticación que requieren la introducción de un pin o una contraseña asociada a la tarjeta y otros un poco más complejos, como la utilización de tarjetas de coordenadas o el envío de un código al teléfono del usuario legítimo.

3. Sistemas de pago mediante moneda electrónica

La moneda electrónica, también denominada moneda digital, es el sustituto electrónico de la moneda física.

3.1. Características ideales de los sistemas de pago con moneda electrónica

Entre las características de la moneda física destacan:

- **Es transferible.** El valor de la moneda se encuentra en sí misma, y por tanto la transferencia de la moneda entre usuarios representa la transferencia del valor. Además, las monedas se pueden utilizar en sucesivos pagos sin necesidad de depositarlas en el banco. El receptor de la moneda tiene, por tanto, la posibilidad de utilizarla en un nuevo pago.

- **Es infalsificable.** La moneda se crea basándose en criterios de seguridad que hacen difícil su falsificación y que permiten la identificación de las copias falsas. Estas medidas de seguridad se basan en características físicas difíciles de imitar, que limitan su reproducción.

- **Es anónima.** Las transacciones con moneda física no requieren la identificación del pagador ni del receptor del pago. Si no hay otros documentos que certifiquen el intercambio, la transacción de la moneda física no vincula a las identidades de los usuarios.

- **Es independiente de terceras partes durante el pago.** Los usuarios pagador y receptor son los únicos involucrados en la etapa de pago. La seguridad en la validez de la moneda física hace que no se requiera la presencia de ninguna tercera parte para validar la transferencia.

Las características ideales de un sistema de pago con moneda electrónica son aquellas que permiten realizar transacciones remotas con las prestaciones de las transacciones con moneda física.

Las características ideales de la moneda electrónica tendrán como punto de partida las características anteriores. A estas características se les añadirán otras específicas, derivadas de la naturaleza digital de las monedas.

1) Independencia. La seguridad de las monedas no debe depender de ninguna característica física. Han de ser transmisibles a través de redes. Las monedas son una cadena de bits.

2) Seguridad. Se debe prevenir la creación de monedas falsas. Por otra parte, también se ha de prevenir (o detectar) el uso de copias de las monedas existentes en pagos (a este fraude se le denomina reutilización).

3) Privacidad. Los pagos han de ser anónimos, la identidad del pagador no debe formar parte del pago, ni de la moneda. No deberá ser posible establecer una conexión entre el pagador y sus compras aunque más de un parte colabore (característica conocida como no rastreabilidad), así como tampoco vincular, entre ellas, las compras realizadas por el mismo usuario (no vinculabilidad).

4) Pago fuera de línea. En un pago fuera de línea (en oposición a en línea), la conexión con el emisor de las monedas, con la finalidad de validación del pago, no es necesaria durante una transferencia de pago. Solo intervienen los usuarios pagador y receptor.

5) Transferibilidad. Un sistema transferible presenta la capacidad de utilizar la misma moneda en transacciones sucesivas sin depositarla y sin la intervención de ninguna tercera parte. Esta propiedad posibilita que un receptor pueda utilizar una moneda recibida para realizar un nuevo pago.

6) Divisibilidad. La divisibilidad es la capacidad de fraccionar la moneda, y por tanto de utilizar diferentes fracciones de la moneda en diferentes pagos, permitiendo así pagos exactos con fracciones o sumas de fracciones que equivalgan al importe del pago. La divisibilidad de la moneda es la alternativa a la vinculación de diferentes monedas en el mismo pago. Permite obtener partes de la moneda de manera que la suma de las partes sea igual al valor de la moneda original. Algunos sistemas que no presentan la característica de divisibilidad implementan la posibilidad de devolver cambio cuando el pago no es exacto.

Estas características ideales son el punto de partida de los sistemas de pago mediante moneda electrónica. La importancia relativa de cada una de ellas dentro del conjunto se fija en función de la aplicación. Además, los sistemas de pago destinados a realizar pagos en los cuales la cantidad involucrada está fuera de un rango de valores determinado, ya sea porque el valor del pago es muy grande o muy pequeño, se considerarán sistemas de pago específicos, y en estos casos se hace necesaria la redefinición de las características ideales.

3.2. Funcionamiento básico de un sistema de pago con moneda electrónica: entidades y procedimientos

En su forma más simple, un sistema de pago con moneda electrónica consiste en un conjunto de cuatro procedimientos que involucran a tres partes: el pagador, el receptor y el banco (o bancos, en caso de que haya diferentes entidades bancarias, y pagador y receptor tengan cuentas en diferentes entidades).

Los procedimientos son:

- **Establecimiento de la cuenta**. Esta operación se realiza una sola vez. En esta etapa se vincula la identidad o el seudónimo del usuario a la nueva cuenta. El usuario dispone de un par de claves correspondientes a un criptosistema asimétrico y de un certificado de clave pública. Determinadas operaciones sobre esta cuenta requerirán el conocimiento de la clave privada del par asociado al certificado del usuario.

- **Obtención de la moneda**. Para obtener la moneda se pueden distinguir varias situaciones en función de si la moneda se extrae de la cuenta del usuario antes del pago o después. En el primer caso se dispone de un sistema de prepago o a débito, mientras que, en el segundo, el sistema funciona a crédito. En un sistema de débito el valor es descontado antes de su utilización en la etapa de pago. El descuento y la creación de la moneda se produce durante la ejecución del procedimiento de reintegro o retirada (este procedimiento requiere la autenticación del usuario).

- **Pago**. El pagador lleva a cabo un pago involucrando una o más monedas. En determinados sistemas, estas monedas son comprobadas por el banco en la misma fase de pago. En otros, el pago solo contiene la transferencia de la moneda entre pagador y receptor. En este segundo caso el receptor podrá comprobar si la moneda es válida pero no podrá verificar si es la copia de una moneda utilizada antes en otra transferencia.

- **Depósito**. Una vez realizado el pago, el usuario que lo ha recibido lo puede hacer efectivo depositando la moneda en su cuenta, aunque en sistemas transferibles también puede optar por transferir la moneda. Si la reutilización de la moneda no ha sido comprobada antes, se hace en esta etapa. También se comprueba que el receptor del pago no deposite dos veces la misma moneda.

Sistema a crédito

La etapa de obtención de la moneda no existe en sistemas a crédito, como se señala en R. Rivest, A. Shamir: Payword and Micromint: two simple micropayment schemes, Fourth Cambridge Workshop on Security Protocols, LNCS 1189, pág. 69-87, Springer Verlag, 1996. En este caso la identificación de la cuenta del pagador se hace durante el depósito.

3.3. Seguridad en sistemas de moneda electrónica

Los sistemas de pago mediante moneda electrónica incluyen mecanismos de seguridad para evitar el fraude relacionado con la falsificación y el uso fraudulento de las monedas. Concretamente, los sistemas previenen o detectan los tipos de fraude siguientes:

- **Falsificación**. La creación de monedas es un derecho exclusivo de alguna de las partes del sistema (por ejemplo, el banco). Habitualmente, los sistemas de moneda electrónica utilizan protocolos en los que la creación de la moneda involucra el conocimiento de algún parámetro secreto que imposibilita la creación de monedas por partes no autorizadas (falsificación), que no conocen el parámetro requerido para la creación de monedas. Una estructura frecuente consiste en incorporar a la moneda una firma digital de la entidad emisora.

- **Reutilización**. Aunque las monedas digitales no puedan ser falsificadas (es decir, no se pueden crear monedas falsas diferentes de las reales), la duplicación de monedas es fácilmente realizable porque solo se requiere la duplicación de la información digital que representa la moneda. A diferencia de la moneda física, la electrónica se puede reutilizar. Por esta razón, los sistemas de pago utilizan algún mecanismo para prevenir, en el mejor de los casos, o como mínimo detectar los casos de reutilización de monedas. El control sobre la reutilización de las monedas no presenta una solución tan satisfactoria como la prevención de la falsificación, ya que los usuarios pueden no disponer de información actualizada sobre el estado de la moneda. Por esta razón, muchos sistemas optan por la detección en lugar de la prevención. La prevención es posible utilizando dispositivos resistentes a manipulación para almacenar las monedas, ya que estos dispositivos no permiten el pago con monedas ya utilizadas. Esta solución puede ser eficaz, aunque costosa, ya que obliga a todos los usuarios a dosponer de un dispositivo y utilizarlo.

  La segunda alternativa para la reutilización consiste en contactar con una tercera parte (que puede ser un banco) durante cada pago (sistema en línea). De esta manera la tercera parte centraliza el conocimiento sobre la utilización de las monedas y puede informar al receptor del pago sobre la validez de la moneda con la que el pagador intenta pagarle.

  Si se opta por no prevenir el ataque, la reutilización de una moneda en el mismo comercio o la repetición de su depósito en el banco puede ser detectada al instante por parte del receptor, pero no podría serlo, por ejemplo, la reutilización de la moneda en diferentes comercios. En este caso la reutilización no se detecta hasta que los dos receptores deciden depositar la moneda. Por funcionalidad, las monedas se crean con el objetivo de que se puedan utilizar en pagos a cualquier usuario (aunque algunos sistemas

de micropago generan monedas específicas para receptores con los que el usuario mantiene relaciones a largo plazo). Si la moneda puede ser utilizada para pagos a diferentes receptores, entonces se deberá solucionar el problema de la reutilización.

En los sistemas en los que los usuarios se identifican durante la etapa de pago, en caso de reutilización se puede identificar fácilmente al usuario infractor.

- **Sobreutilización**. Los sistemas de pago deben garantizar que todas las monedas creadas representen dinero existente en la cuenta del usuario. Es decir, las monedas representan dinero real.

  Los sistemas a crédito, en los que el usuario es el creador de la moneda, pueden sufrir sobreutilización. Cuando la moneda, después del pago, es depositada por el receptor, se puede encontrar con la falta de fondos en la cuenta del pagador. En los sistemas de débito, las medidas adoptadas para la prevención de la falsificación previenen la sobreutilización de las monedas.

3.4. Sistemas en línea y fuera de línea

En función del mecanismo utilizado para afrontar el problema de la reutilización, los sistemas de pago pueden validar la moneda en el momento de la transferencia (sistema en línea) o verificarla en el depósito (sistema fuera de línea).

En ambos tipos de sistemas, el primer paso es la obtención de la moneda. La transferencia entre pagador y receptor, en cambio, dependerá del tipo de sistema. A continuación se describen estas etapas cuando no se ofrece privacidad; más adelante, se analiza el anonimato en los dos tipos de sistemas.

3.4.1. Creación y obtención de la moneda en un sistema en línea o fuera de línea no anónimo

En la creación de la moneda y la obtención de esta por parte del usuario, el primer paso consiste en la solicitud de obtención enviada por el usuario al banco. Con esta solicitud, el usuario espera obtener una moneda a cambio del decremento por el valor de la moneda en su cuenta. Esta es una operación en la que se debe asegurar que el solicitante es efectivamente el titular de la cuenta. Por este motivo la solicitud de creación y obtención de moneda se envía firmada al banco.

A continuación, el banco crea la moneda utilizando algún parámetro secreto, por ejemplo firmando la moneda utilizando su clave privada, para prevenir la falsificación de monedas. La moneda incluirá su valor y puede incluir una fecha de caducidad.

Finalmente, el banco envía la moneda al usuario y descuenta el importe de la cuenta del usuario. El banco está autorizado a decrementar la cuenta de un usuario únicamente cuando dispone de una solicitud autenticada que lo autoriza a hacerlo. Si esta solicitud incluye el valor solicitado, el banco solo puede decrementar la cuenta del usuario en la cantidad indicada. Además, el banco no podrá utilizar dos veces la misma solicitud si hay algún parámetro que identifique la solicitud (como un número de serie).

Con este procedimiento el banco conoce, a la vez, la moneda y al usuario a quien la ha enviado. Los pagos realizados con la moneda no serán anónimos. Se podrá reconocer al usuario a partir de la identificación de la moneda, ya que esta está directamente relacionada con la identidad o la cuenta del usuario que la solicitó.

3.4.2. Pago en un sistema en línea no anónimo

En los sistemas en línea, y para prevenir las reutilizaciones, el banco mantiene una base de datos con los números de serie de las monedas utilizadas. En todos los pagos el receptor solicita al banco la comprobación de la moneda antes de aceptarla. Es decir, se requiere la participación de la tercera parte (banco) en la etapa de pago. En caso de reutilización (la moneda ya ha sido utilizada previamente, y su identificador se encuentra en la lista), se rechaza el pago. En cambio, si la moneda no está en la base de datos en el momento del pago, el banco permite al receptor aceptar el pago. En este momento la moneda se incorpora a la base de datos de monedas utilizadas.

3.4.3. Pago en un sistema fuera de línea no anónimo

En los sistemas fuera de línea no se hace la comprobación de la validez de la moneda durante el pago. Los sistemas fuera de línea que no utilizan dispositivos resistentes a manipulación para prevenir la reutilización afrontan el problema desde la perspectiva de la detección e identificación de los reutilizadores. La infracción se detecta después del segundo depósito de una misma moneda. El paso siguiente es la identificación del infractor cuando la reutilización ya se ha producido. La identificación del infractor es sencilla si la identidad del pagador está incluida dentro de la información relacionada con el pago, o está incluida dentro de la moneda. No es necesario que la identidad del pagador aparezca de manera explícita para poder realizar la identificación del reutilizador, es decir, no es necesario que aparezca directamente el nom-

bre del usuario o su número de cuenta. Si un usuario esconde su identidad detrás de un seudónimo, la identificación se podrá llevar a cabo por parte de la entidad emisora del seudónimo, que puede relacionar la información no identificadora (seudónimo) con la identidad del usuario.

3.5. Privacidad en sistemas de moneda electrónica: anonimato y no-rastreabilidad

Se considera una característica deseable de todo sistema de pago la posibilidad de que el pagador permanezca anónimo frente al receptor, y un requisito todavía más estricto, que el pagador permanezca anónimo también frente a terceras partes y, por tanto, no se lo pueda vincular posteriormente con la compra realizada.

Un sistema será no rastreable si la confabulación de las restantes partes no puede desvelar la relación entre la identidad del usuario pagador y el uso dado a las monedas electrónicas.

Si, aunque no se revele la identidad del usuario, los pagos hechos por el propio usuario (o la misma pareja pagador-receptor) se pueden vincular, se dirá que el sistema es vinculable.

En un sistema totalmente anónimo, además de ocultarse la identidad del usuario durante el pago, se deberían garantizar la no-rastreabilidad y la no-vinculabilidad. En un sistema vinculable, se corre el peligro de que la identificación de un usuario en un único pago permita desvelar la totalidad de los pagos realizados por este usuario.

El uso de seudónimos permite ocultar la identidad al resto de las partes del sistema, excepto al emisor de seudónimos. Este emisor podría desvelar la relación entre identidades y seudónimos, con lo que se destruiría el anonimato del sistema.

En los sistemas de moneda electrónica, el anonimato dependerá, entre otros factores, de la técnica utilizada en la creación de la moneda. Si durante la creación de la moneda y su posterior emisión el banco puede registrar una característica de la moneda como su número de serie y vincularla al usuario, aunque este después no se identifique durante el pago, el sistema no será anónimo en sentido estricto. Cuando el receptor deposite el pago, el banco podrá reconocer la moneda e informar al receptor de cuál es la identidad del pagador: en este caso el sistema es rastreable.

Los sistemas no rastreables utilizan técnicas de creación de moneda que permiten que el banco emita monedas válidas sin conocer ninguna característica de ellas que sirva para reconocerlas posteriormente.

Como conclusión, establecemos las siguientes categorías de anonomato de más laxa a más estricta.

- Seudónimos. En los sistemas donde se utilizan seudónimos, las operaciones identificadas utilizan el seudónimo, de manera que no se revela directamente la identidad del usuario. Todas las operaciones realizadas por el mismo usuario utilizarán el mismo seudónimo y pueden ser vinculadas. Si se conoce la identidad del usuario en una única operación, este conocimiento permite identificar todas las operaciones realizadas por este usuario.

- Anonimato rastreable. En los sistemas anónimos rastreables, la identidad del pagador no aparece en las operaciones de pago y, por tanto, la otra parte involucrada en la transferencia no conoce la identidad de su interlocutor. Esta circunstancia cambia cuando se utiliza el conocimiento del que disponen dos o más partes (por ejemplo, el receptor del pago y el banco que generó la moneda). Una confabulación de las partes puede revelar la identidad del usuario que ha participado en un pago anónimo.

- Anonimato no rastreable. A diferencia del caso anterior, en un sistema no rastreable, el anonimato no se puede revocar por la adición de los conocimientos de los que disponen dos o más partes. Un usuario puede realizar pagos anónimos con la certeza de que no será identificado a no ser que cometa fraude o actividades delictivas.

- Anonimato no rastreable ni vinculable. Con la propiedad de no-rastreabilidad se garantiza que la identidad de los usuarios no se revelará. Además, si no es vinculable, el conjunto de las operaciones realizadas por un mismo usuario anónimo no se pueden vincular. La vinculación permitiría obtener el perfil de usuarios anónimos.

  A pesar de ser una característica deseable, solo algunos sistemas de pago con monedo electrónica permiten que el usuario realice compras de manera totalmente anónima.

Otro aspecto raramente considerado es el anonimato del usuario que actúa como receptor. Igualmente, hay que proteger la intimidad de la parte que recibe el pago, y ha de ser imposible determinar las fuentes de ingresos de los usuarios receptores. En el anonimato del receptor se pueden distinguir las mismas categorías: el uso de seudónimos, el anonimato únicamente frente al pagador (anonimato rastreable) y el anonimato que permite que banco y pagador

no puedan vincular al receptor con la fuente de sus ingresos (anonimato no rastreable).

3.5.1. Sistema en línea anónimo

Firma ciega

La firma digital ciega es un protocolo de firma digital creado por David Chaum, que permite a una persona obtener un mensaje firmado por una entidad, sin que sea necesario desvelarle el contenido del mensaje que se debe firmar.

La obtención de la moneda en el sistema en línea anónimo es ligeramente diferente que en el sistema en línea identificado. La alternativa más habitual es el uso de firmas ciegas en el proceso de creación de la moneda. De esta manera, el banco no reconoce la moneda que ha creado y, aunque en el depósito podrá validar la moneda verificando la firma, no podrá relacionar la moneda con el usuario que la solicitó.

3.5.2. Sistema fuera de línea anónimo

En los sistemas fuera de línea anónimos, a diferencia de los sistemas fuera de línea no anónimos, la identificación del reutilizador no se puede hacer directamente: el pago se limita a la transmisión de una moneda anónima. Si se opta por prevenir la reutilización, un mecanismo consiste en el uso de dispositivos resistentes a manipulación que impiden el uso de una moneda en diferentes pagos. Estos dispositivos resistentes a manipulación hacen una prevención de la reutilización, pero su incorporación en los sistemas afecta a la viabilidad del sistema, ya que implica que cada usuario tenga un dispositivo para poder efectuar los pagos.

Si, en cambio, se opta por la detección, hay varias soluciones para conseguir la identificación. La solución adoptada más frecuentemente en los sistemas fuera de línea anónimos (que no utilizan dispositivos resistentes a manipulación) es la revocación del anonimato en caso de detección de reutilización. De esta manera, el pagador se mantiene anónimo en el caso general, siempre que no se reutiliza la moneda, mientras que en caso de reutilización, dos pagos diferentes se podrán utilizar para revelar la identidad del usuario infractor.

Esta identificación es posible gracias a la inclusión en el protocolo de pago de una etapa de reto-respuesta en la que el receptor del pago envía un reto al pagador y espera obtener una respuesta. El reto se forma a partir de datos aleatorios. La respuesta se firma a partir de información identificadora del usuario, pero donde esta se mantiene oculta. Si se reutiliza la moneda, entonces los receptores dispondrán de dos respuestas a dos retos diferentes. Estas respuestas permitirán revelar la información identificadora del pagador que se mantenía oculta en cada una de las respuestas cuando estas se presentaban de manera separada (Brands, 1993; Chaum, 1988).

La inclusión de información oculta se puede realizar mediante diferentes técnicas. Esta información permanecerá oculta y no podrá ser utilizada para revocar el anonimato de los usuarios que hagan un uso correcto de las monedas.

Durante la creación de la moneda, la entidad emisora se debe asegurar de que esta información oculta realmente está incluida en la moneda. Posteriormente, si se confirma un caso de reutilización se dispondrá de suficiente información para revelar la identidad del usuario infractor. Cualquier otra situación, como un doble depósito por parte del receptor del pago, se debe detectar (Brands, 1993) y no podrá ser utilizada para revocar el anonimato del pagador.

Métodos de identificación

Los métodos ***cut and choose*** y ***single term*** permiten incluir en las monedas información relacionada con la identidad del usuario.

3.5.3. Descripción de un sistema fuera de línea anónimo

El sistema de pagos anónimos presentado en Chaum (1988) permite identificar a los usuarios en caso de reutilización. El sistema utiliza la firma RSA para la creación de las monedas. Estas podrían ser de la forma $(x, f(x)^{1/3} \pmod n)$, donde n es un valor cuya factorización es conocida solo por el banco y f es una función unidireccional adecuada.

El protocolo para la expedición y el uso de este dinero se puede resumir de la manera siguiente:

1) Alice elige los aleatorios x y r, y envía al banco $B = r^3 f(x) \pmod n$. Alice solicita un dólar al banco.

2) El banco devuelve la raíz cúbica de B módulo n: $r^* f(x)^{1/3} \pmod n$ y retira un dólar de su cuenta.

3) Alice extrae $C = f(x)^{1/3} \pmod n$ de B, ya que conoce el valor de r.

4) Para pagar un dólar a Bob, Alice le da el par $(x, f(x)^{1/3} \pmod n)$

5) Bob inmediatamente contacta con el banco, verificando que esta moneda electrónica no ha sido depositada antes.

Se puede comprobar fácilmente que la moneda tiene la estructura correcta y ha sido firmada por el banco, pero el banco no puede vincular esta moneda específica a la cuenta de Alice.

Entre otras ventajas, el enfoque de la propuesta que se desarrollará a continuación elimina el requisito de que el comerciante se haya de comunicar con el banco durante cada transacción. Si Alice utiliza una moneda una sola vez, su privacidad está protegida incondicionalmente. Pero si Alice reutiliza una moneda, el banco puede rastrear su cuenta y se puede demostar que la ha utilizado dos veces. Para hacerlo, el protocolo utiliza el método *cut & choose*. A continuación se presenta el esquema básico, que garantiza la imposibilidad de rastreo, pero permite al banco trazar un reutilizador.

Monedas no rastreables

El banco publica inicialmente un RSA módulo n, cuya factorización se mantiene en secreto y para el que $\phi(n)$ no tiene factores pequeños. El banco también establece un parámetro de seguridad k.

Sean f y g funciones de dos argumentos libres de colisiones. Alice tiene una cuenta bancaria numerada u y el banco mantiene un contador asociado v. $\oplus$ denota una or exclusiva bit a bit y $\|$ denota la concatenación.

OBTENCIÓN: Para tener una moneda electrónica, Alice sigue el protocolo siguiente con el banco:

1) Alice elige a_i, c_i y d_i, $1 \leqslant y \leqslant k$, de manera independiente y uniforme al azar a partir de los residuos (mod n).

2) Alice forma y envía al banco k candidatos encegados (denominados B).

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

donde

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

y

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

3) El banco elige al azar un subconjunto de k / 2 candidatos encegados $R = i_j$, $1 \leqslant i_j \leqslant k/2$ y lo transmite a Alice.

4) Alice muestra los valores de r_i, a_i, c_i, y d_i, para todos los i de R, y el banco los comprueba. Recordad que $u \| (v + i)$ es conocido por el banco. Para simplificar la notación supondremos que R = {k/2+1, k/2+2,. ,. , K}.

5) El banco da a Alice $\Pi\ B_i^{1/3}$ para todos los i que no pertenecen a R, es decir $\Pi\ B_i^{1/3}$ mod n para los valores $1 \leqslant y \leqslant k/2$ y carga un dólar en la cuenta de Alice. El banco también incrementa el contador de Alice k unidades.

6) Alice entonces puede extraer fácilmente la moneda electrónica

$$C = \Pi\ f(x_i, y_i)^{1/3} \bmod n \text{ para los valores de i entre 1 y k/2.}$$

Alice reindexa los candidatos 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 también incrementa su copia del contador, v, k unidades.

Pago: Para pagar 1 $ a Bob, Alice y Bob proceden de la manera siguiente:

1) Alice envía a Bob el elemento C.

2) Bob elige al azar una cadena binaria z_1, z_2, z_3,... $z_{k/2}$.

3) Alice responde de la siguiente manera, para todo $1 \leqslant y \leqslant k/2$:

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

4) Bob verifica que C es de la forma adecuada y que las respuestas de Alice encajan con C.

5) Bob después envía C y las respuestas de Alice al banco, que verifica su corrección e incrementa el crédito de su cuenta.

El banco debe almacenar C, la cadena binaria z_i, ..., z_k y los valores de a_i (para $z_i = 1$) y $a_i \oplus (u \| (v+i))$ (para $z_i=0$).

Detección de reutilización. Si Alice utiliza la misma moneda C dos veces, entonces tiene una alta probabilidad de ser trazada: con alta probabilidad, dos tenderos diferentes habrán enviado valores binarios complementarios para el menos un bit z_i. El banco puede buscar fácilmente sus registros para asegurarse de que C no se ha utilizado antes. Si Alice utiliza C dos veces, entonces, con alta probabilidad, el banco tiene tanto a_i como $a_i \oplus (u \| (v+i))$. Por tanto, el banco puede aislar y rastrear el pago hasta la cuenta de Alice.

Un posible problema con este sistema es una confabulación entre Alice y un segundo tendero, Charlie. Después de la transacción con Bob, Alice describe la transacción a Charlie, y tanto Bob como Charlie envían al banco la misma información. El banco sabe que con una probabilidad muy alta uno de ellos está mintiendo, pero no tiene manera de saber quién, y no se puede rastrear la moneda hasta la cuenta de Alice.

Mediante la fijación del reto de Bob a Alice, se puede evitar que esta confabulación defraude al banco. Cada comerciante tiene una cadena de consulta fija. Para evitar la reutilización por parte de Alice de la misma moneda, parte del reto de la misma tienda aún ha de ser calculado al azar.

3.6. Control de anonimato: revocación

La posibilidad de efectuar pagos de manera anónima tiene como consecuencia la posibilidad de llevar a cabo actividades ilícitas, ya que el usuario infractor puede permancer anónimo. Entre estas actividades se encuentra el blanqueo

de dinero, la extorsión o chantaje, la venta de productos ilegales y la compra de estos productos.

Blanqueo

El blanqueo es posible si un usuario puede esconder el origen de sus ingresos y utilizarlos anónimamente.

Compra-venta de productos ilegales

El anonimato del pagador permite que un usuario pueda adquirir productos ilegales con la certeza de no ser identificado. De la misma manera, el anonimato del receptor permite la venta de estos productos.

Extorsión y chantaje

Un usuario extorsionador puede exigir que se le den unas determinadas monedas que después pueda gastar anónimamente.

3.6.1. Técnicas de control de anonimato

Una vez que el anonimato puede dar lugar a actividades ilícitas se cuestiona su conveniencia. A favor está la protección de la intimidad del usuario pagador y su derecho a realizar compras de manera anónima. La contrapartida es la posible proliferación de las actividades ilícitas indicadas anteriormente. La solución general es adoptar una política de control de anonimato. De la misma manera que algunos sistemas con detección *a posteriori* de la moneda permiten revocar el anonimato del usuario infractor, los sistemas con control de anonimato permiten identificar a los usuarios solo cuando se demuestra o se sospecha que están involucrados en alguna actividad ilícita.

La revocación del anonimato es realizada por una tercera parte de confianza (TTP) cuando se determina que el usuario ha infringido la ley. En función del sistema, esta tercera parte deberá estar presente en todas las etapas del pago o será suficiente que participe únicamente en algunas de ellas. En sistemas eficientes se requiere la participación de la TTP durante la retirada de la moneda, pero no durante el pago, y solo se solicita su participación en caso de necesidad de revocación.

No todas las actividades ilícitas necesitan el mismo tipo de algoritmo de revocación. Por ejemplo, un caso de chantaje requiere reconocer la moneda cuando esta sea utilizada en el futuro para revocar la identidad del extorsiona-

dor. Otras, como el blanqueo, necesitan identificar las fuentes de ingresos del usuario inspeccionado.

Basándose en estas dos necesidades se crean los algoritmos de seguimiento de moneda (*coin tracing*) y de seguimiento de usuario (*owner tracing*).

- *Coin tracing*. Los algoritmos de seguimiento de moneda permiten, dada una moneda determinada en su creación, seguir su rastro. De este modo se puede identificar a un chantajista encontrando el destino de las monedas que ha recibido como resultado del chantaje. Cuando el chantajista intenta gastar la moneda (en sistemas transferibles) o depositarla, se iniciaría su identificación revocando su anonimato.

- *Owner tracing*. Los protocolos de este tipo identifican al poseedor de una determinada moneda después de que se realice el pago. Serán útiles para detectar el blanqueo y las compras ilegales, ya que permiten identificar el origen de las monedas dudosas. Su objetivo es permitir rastrear los pagos una vez realizados. También permite identificar a los compradores de productos ilegales una vez identificado el receptor.

3.6.2. Características ideales del control de anonimato

Las características de los sistemas de revocación del anonimato se determinan con criterios de eficiencia y de privacidad, ya que la revocación no debería ser posible sin la certeza de la culpabilidad del usuario.

- La revocación es una capacidad exclusiva de una tercera parte de confianza (TTP).

  Ni los pagadores, ni los receptores, ni el banco, ni ninguna combinación de ellos debe poder reconocer una determinada moneda (vinculada con una operación concreta) o revelar la identidad del propietario si no es en caso de reutilización o de actividad ilícita.

- La TTP actúa fuera de línea.

  Por el mismo motivo que en las características ideales generales de los pagos se indica que el banco debe actuar fuera de línea, ahora se considera deseable que la TTP no intervenga en los pagos ni en la obtención de la moneda ni en su depósito.

- La TTP solo actúa cuando se requiere legalmente.

  No se pierde el anonimato en el caso general. Para los usuarios que actúen correctamente el sistema continúa siendo anónimo. Estos usuarios deben

tener la certeza de que no se revelará su identidad. Por este motivo se deben presentar pruebas o una orden emitida por una autoridad para poder iniciar la revocación.

- La capacidad de la TTP puede estar distribuida entre diferentes entidades.

  La confianza de los usuarios en la TTP es un punto crítico del sistema. Por este motivo, se puede decidir distribuir esta confianza en un grupo de TTP, de manera que solo la colaboración de todas ellas (o de un subconjunto) permita revocar el anonimato.

4. Sistemas de micropago

Los sistemas de micropago se adaptan a las necesidades de los pagos de cantidades muy pequeñas, y por esta razón presentan una serie de características diferenciadoras de los sistemas de pago mediante moneda electrónica pensados para pagos de cantidades mayores.

4.1. Motivaciones

Las aplicaciones recientes del comercio electrónico presentan un reto para los sistemas de pago electrónico existentes. Las ventas que involucran el pago de pequeñas cantidades y las ventas de productos que se pueden ofrecer a través de la red presentan características especiales que la mayoría de los sistemas de pago no pueden satisfacer. El motivo se encuentra en el margen de beneficio del pago de una cantidad pequeña. Este no permite utilizar sistemas en los que el coste asociado se pueda acercar a este margen, o incluso superarlo. Los sistemas de micropago se adaptan a los requisitos de los pagos de pequeñas cantidades, en especial al requisito de eficiencia, que permite costes asociados reducidos.

Los micropagos son especialmente útiles en la compra de información. La información es un bien que se puede ofrecer a través de la red, es decir, permite hacer un intercambio instantáneo entre el bien y la moneda electrónica. La información se puede vender en diferentes volúmenes, por lo que se deberá facilitar la compra y el pago de pequeñas fracciones de información. Las monedas electrónicas permitirían hacer pagos de cantidades de información moderadas a grandes, pero sus costes asociados harían poco viable la compra de pequeños volúmenes de información. Por ejemplo, se puede utilizar una moneda electrónica para pagar la visualización de la edición electrónica de un diario completo, pero no para pagar la visualización de un artículo concreto de este diario, con un coste mucho menor. El precio de este artículo podría estar por debajo del coste mínimo por transferencia asociado al sistema de pago con moneda electrónica.

Además, hay que tener en cuenta que la posibilidad de ofrecer el producto en línea elimina los costes logísticos y permite vender a un precio inferior. Entre los servicios ofrecidos actualmente se encuentran múltiples aplicaciones de la compra de información, como visualización de contenidos de páginas web, compras de archivos musicales, acceso a artículos de prensa, consultas de enciclopedias, descarga de software de prueba, acceso a archivos de fotos, mapas o directorios telefónicos, consultas en buscadores, etc.

4.2. Alternativas a los micropagos

Actualmente, y hasta que se generalice el uso de los micropagos, la información se ofrece utilizando alternativas al pago exacto e instantáneo de la información consumida. Entre estas alternativas encontramos:

1) Acceso gratuito a la información. La primera alternativa consiste en publicar la información permitiendo un acceso gratuito a esta. Esta alternativa no presenta una solución general, ya que los poseedores de los derechos de propiedad intelectual de determinados recursos están poco motivados a hacerlos accesibles de esta manera. De aquí se deriva que parte de estos recursos no estén disponibles para su consumo en línea.

2) Publicidad como fuente de ingresos. Después del acceso gratuito, sin beneficios para el propietario, otra alternativa ampliamente utilizada consiste en obtener una fuente de ingresos (que subvencione la publicación de la información) diferente del usuario que la consume. Las barras publicitarias se insertan en los documentos que contienen la información o permiten su descarga. La empresa anunciadora hace el pago que permitirá el acceso gratuito a la información a cambio de la visualización de la publicidad. Algunas de las implementaciones de esta alternativa presentan problemas respecto a la protección de la intimidad de los usuarios, ya que las empresas anunciadoras o las empresas que gestionan la publicidad de terceros utilizan técnicas para la personalización de la publicidad que recibe el usuario, basándose en información recogida de sus hábitos de navegación.

3) Suscripciones. La tercera posibilidad consiste en pagar por un volumen de información grande, que se irá consumiendo con el tiempo, es decir, una suscripción. Podemos encontrar dos tipos de suscripciones: temporales y por accesos. Una suscripción temporal permite el acceso del usuario a la información durante un periodo de tiempo determinado. A diferencia de la suscripción temporal, una por volumen de información permitirá al usuario acceder a información mientras tenga crédito con la fuente de información, procedente del pago inicial. El crédito inicial se irá decrementando en cada acceso, independientemente del momento en el que este se haga.

Ninguna de estas alternativas es ideal, ni para el usuario ni para el propietario de la información. Las dos primeras alternativas permiten al usuario acceder gratuitamente a la información, pero no permiten al propietario de la información cobrar por volumen de información consumida. Por otra parte, las suscripciones obligan al usuario a pagar por un volumen de información que quizá no llegará a consumir, y a hacer una inversión inicial. Desde el punto de vista del usuario, realizar el pago de la cantidad precisa que se consume es la mejor alternativa.

4.3. Características ideales de los sistemas de micropago

Las características ideales de los sistemas de micropago difieren, en parte, de las consideradas ideales para los sistemas de macropago, y son las siguientes:

- **Costes por transferencia reducidos**. El coste de las microtransferencias deberá representar una pequeña fracción del valor involucrado en el pago. Este es un requisito muy exigente en los micropagos. Su cumplimiento tiene como contrapartida, habitualmente, la relajación o el incumplimiento de las otras características ideales.

- **Límite inferior**. El límite inferior deberá ser suficientemente pequeño para permitir transferencias del orden de un céntimo de euro para adaptarse a los pagos por pequeños volúmenes de información.

- **Control de riesgos financieros**. En los micropagos, los mecanismos de seguridad utilizados para evitar el fraude se limitan para garantizar la eficiencia y mantener los costes por transferencia en un nivel aceptable. La reducción de los mecanismos de seguridad supone la aparición de ciertos riesgos financieros. Los riesgos asumidos por cualquier sistema de micropago se deben mantener controlados y limitados.

- **Intercambio atómico**. En la compra de los bienes que se pueden ofrecer a través de la red, es deseable la realización del pago de manera atómica con la transferencia del bien, de modo que el intercambio sea equitativo.

- **Velocidad**. La transferencia debe ser bastante rápida para adaptarse al microcomercio y para permitir un gran número de operaciones por sesión con el servidor.

- **Privacidad**. La protección de la intimidad se considera una característica ideal para cualquier sistema de pago. En general, los aspectos relacionados con la privacidad se oponen a la eficiencia. Este hecho es especialmente importante en los sistemas de micropago a causa de los altos requisitos de eficiencia que estos tienen.

4.4. Necesidad de reducción de los costes

La eficiencia en los micropagos que nos permitirá aceptar pagos para cantidades muy pequeñas se obtiene reduciendo los costes asociados al pago ocasionados por diferentes factores.

Los costes se pueden relacionar con:

- Costes de control de riesgos financieros: medidas de seguridad utilizadas para combatir el fraude.
- Costes de comunicación: número de interacciones y volumen de información transferida.
- Costes de procesamiento de datos.
- Costes relacionados con el uso que se da a la moneda: moneda genérica o específica.
- Costes de almacenamiento.
- Costes de mantenimiento de privacidad y anonimato.
- Costes derivados del uso de dispositivos resistentes a manipulación.

Esta reducción de costes se puede concretar en cuatro puntos:

1) Eliminar computación en línea

En los sistemas de pago electrónico, la etapa de pago se puede realizar con la intervención del banco o sin ella. Eliminando la vinculación del banco en la etapa de pago se reduce el coste de comunicación. Por otra parte, los sistemas fuera de línea permiten transferencias más rápidas y con menos operaciones. Como contrapartida, los sistemas fuera de línea pueden sufrir reutilización. La prevención de la reutilización de monedas se podría efectuar con el uso de dispositivos resistentes a manipulación, como son las tarjetas inteligentes. Aunque estas pueden hacer las funciones del banco de manera distribuida, se descarta su uso en los micropagos porque introducen el coste adicional de su mantenimiento. Por este motivo los sistemas de micropago tienden a introducir el uso de moneda específica como medida de prevención de la reutilización.

2) Minimización del uso de criptografía asimétrica

En los sistemas de pago con moneda electrónica, la criptografía asimétrica se combina con la criptografía simétrica y las funciones de *hash*. La criptografía asimétrica permite realizar tareas de identificación y autenticación de usuarios. La creación de monedas (por parte del banco en los sistemas a débito) implica en buena parte de los casos el uso de criptografía asimétrica. Al considerar el uso de estas funciones en los sistemas de micropago encontramos unos costes asociados elevados. Estos costes son de diferentes tipos y son provocados por distintas causas.

Uso de certificados: la verificación de firmas, así como otras operaciones realizadas con criptografía asimétrica, requieren el uso del correspondiente certificado de clave pública. Los certificados deben ser emitidos por una tercera parte de confianza y renovados periódicamente. También se han de gestionar las listas de revocación de los certificados.

Computación intensiva: los algoritmos de encriptación y desencriptación de los criptosistemas de clave pública tienen un coste computacional superior

al de los algoritmos de clave secreta. Aun así, la criptografía asimétrica no desaparece en todos los sistemas de micropago. En los que se mantiene, las costosas operaciones se amortizan sobre varios micropagos para distribuir el coste computacional y mantenerlo limitado.

3) Suprimir el anonimato y la privacidad

Los sistemas anónimos utilizan mayoritariamente criptografía asimétrica. En el punto anterior se describen las causas que hacen recomendable la minimización del uso de la criptografía asimétrica. Con el objetivo de minimizar las operaciones realizadas con criptografía asimétrica, el anonimato se considera una característica prescindible, en favor de la eficiencia. Normalmente no se incluye el anonimato en los sistemas para micropagos. En los sistemas en los que se considera el anonimato, el coste computacional correspondiente a cada pago se acerca al coste de los pagos con moneda electrónica, haciéndolo no factible para su utilización en micropagos.

4) Uso de moneda específica

Las monedas específicas solo pueden ser utilizadas con un receptor determinado. Vinculan tanto al emisor como al receptor del pago (en determinados casos solo vinculan al receptor) y suponen el establecimiento de relaciones a largo plazo, ya que la generación eficiente de moneda específica se basa en la creación de conjuntos de monedas que serán utilizadas para pagos al mismo receptor.

4.5. Descripción de un sistema de micropago

En esta sección se describirá un sistema de micropago: el sistema payword descrito por Rivest y Shamir (1996).

Payword es un sistema de micropago en el que las partes son brokers, usuarios pagadores y vendedores o proveedores. Los brokers autorizan a los usuarios a realizar micropagos y aceptan los pagos recibidos por los vendedores. El broker mantiene relaciones a largo plazo con usuarios y vendedores.

Payword es un sistema basado en crédito y optimizado por secuencias de micropagos. Su funcionamiento se basa en las fases siguientes:

1) Un usuario crea una cuenta con un broker, que proporciona al usuario un certificado firmado digitalmente. Este certificado autoriza al usuario a hacer cadenas de paywords, que son cadenas de valores de *hash*.

2) Antes de contactar con un proveedor o vendedor, el usuario crea fuera de línea una cadena de paywords específica de su proveedor.

3) El usuario autentica la cadena completa al proveedor con una sola firma mediante un sistema de clave pública y después, sucesivamente, revela cada payword de la cadena para hacer cada micropago.

4) El vendedor cobra los paywords recibidos del usuario con el broker original.

Cadenas de paywords

En la construcción de una cadena payword se utiliza una función *hash* unidireccional, tal como MD5. La función de *hash* h tiene la propiedad de que, dado un valor *y*, es difícil encontrar una entrada *x*, tal que y = h (x).

Un usuario crea una cadena payword $\{W_0, w_1, w_2, ..., w_n\}$ eligiendo el payword final w_n al azar y calculando los otros paywords a través de la función de *hash* w_i = h (w(i+1)). El primer payword w_0 se denomina la raíz de la cadena. Dado w_0 es difícil para cualquier persona que no sea el usuario calcular el resto de los paywords de la cadena.

Relación usuario-broker

Un usuario inicia una relación con un broker al solicitar una cuenta y un certificado payword. El usuario da primero mediante una conexión segura autenticada: su número de tarjeta de crédito, su clave pública PK_U, y su "dirección de entrega" (por ejemplo, dirección IP). El broker, a continuación, emite un certificado firmado digitalmente que autoriza al usuario a hacer cadenas payword hasta una fecha de vencimiento determinada, y autoriza la entrega de bienes solo en la dirección de entrega especificada.

El certificado de usuario, C_U, tiene la forma siguiente: C_U = { broker, usuario, dirección de entrega del usuario, PK_U, fecha de expiración, otra información $_{SKB}$, donde SK_B denota que el contenido de {} está firmado con la clave privada del broker, SK_B.

El certificado C_U es una declaración del broker para cualquier proveedor que autentica los paywords producidos por el usuario y que sean utilizados antes de la fecha de vencimiento, asegurando su cobro.

Relación usuario-vendedor

Las relaciones entre el usuario y el vendedor son transitorias. Un usuario podría visitar un sitio web, comprar diez páginas y después pasar a comprar en

otros sitios. Cuando el usuario contacta con un nuevo proveedor, calcula una nueva cadena payword {W_0, w_1, w_2, ..., w_n}. Aquí el valor de *n* se elige según la conveniencia del usuario; podría ser diez o diez mil.

A continuación, el usuario calcula su compromiso para la cadena: M = {vendedor, C_U, W_0, fecha actual, otras informaciones} $_{SKU}$.

El compromiso M, que se firma con la clave privada del usuario SK_U, autoriza al broker a pagar al vendedor por cualquiera de los paywords w_1, w_2, ..., w_n.

Los paywords son específicos de su proveedor y específicos del usuario que los ha creado; no tienen ningún valor para otro proveedor. Al recibir el compromiso M, el proveedor verifica la firma del usuario en M y la firma del broker en C_U (contenido dentro de M), y comprueba la fecha de vencimiento. Además del compromiso, el pago de un usuario a un proveedor consta de un payword y su índice: (w_i, i). El pago no está firmado por el usuario.

El usuario pasa sus paywords en orden: w_1 primero, y después w_2, y así sucesivamente. Si cada payword vale un céntimo y cada página web cuesta un céntimo, da a conocer al proveedor w_i al pedir su i-ésima página web del proveedor de este día.

Esto conduce a la política de pago payword: para cada compromiso al vendedor se le paga un céntimo, siendo (w_L, L) el pago recibido con un mayor índice. Esto significa que el proveedor necesita almacenar un único pago de cada usuario: el que tiene el índice más alto. El broker puede determinar el valor que va a ser pagado por w_L determinando cuántas veces se ha de aplicar la función de *hash* h sobre w_L para obtener W_0.

Relación vendedor-broker

Un vendedor o proveedor no necesita tener una relación anterior con un broker, pero necesita obtener la clave pública de este de una manera autenticada para poder autenticar certificados firmados por él. También necesita establecer un modo para que el broker le pague los paywords recibidos.

Al final de cada día (o del periodo adecuado), el proveedor envía un mensaje al broker por cada uno de los usuarios del broker que ha pagado al proveedor este día, los compromisos C_U y el último pago P = (w_L, L). El broker necesita primero verificar cada compromiso recibido comprobando las firmas de los usuarios. A continuación, comprueba cada pago (w_L, L) aplicando la función de *hash* L veces.

5. Características adicionales: transferibilidad y atomicidad

En este capítulo se presentan dos características adicionales que permitirían dotar los sistemas de pago de más prestaciones. Se trata de la transferibilidad y la atomicidad.

5.1. Transferibilidad en sistemas de moneda electrónica

La transferibilidad es una de las características de la moneda física y, por tanto, una característica deseable en los sistemas de moneda electrónica.

En los sistemas transferibles, las monedas pueden ser transferidas múltiples veces entre usuarios, sin la necesidad de una verificación en línea por parte de una tercera parte de confianza, y sin haber de ser depositadas.

Se puede decir que la transferibilidad es la generalización del pago fuera de línea, ya que un protocolo transferible contiene los mismos subprotocolos que un protocolo fuera de línea, con la diferencia de que el subprotocolo de transferencia o pago se puede ejecutar múltiples veces entre la retirada y el depósito.

La solución al problema de la reutilización, adoptada en muchos sistemas fuera de línea anónimos, es la de incluir en los pagos alguna información sobre el pagador. Estos sistemas permiten las reutilizaciones en la etapa de pago y las detectan más tarde durante el depósito de la moneda. Si el pagador usa la moneda solo una vez, la información de identificación incluida en ella no permite hacer la identificación, pero si se reutiliza la moneda, la información revelada en dos pagos se puede utilizar para identificar al reutilizador. Los sistemas anónimos transferibles, como generalización de los sistemas fuera de línea anónimos, utilizarán las mismas técnicas de identificación de reutilizadores, pero ahora se aplicarán a todos los usuarios que realicen pagos con la moneda.

5.2. Incorporación de atomicidad en los protocolos de pago electrónico

En una compra electrónica se hace un intercambio siempre que se utiliza un medio de pago electrónico a cambio de un bien o servicio adquirido en un establecimiento electrónico.

A menudo se habla de la atomicidad como una característica deseable para los sistemas de pago electrónico. Posibles fallos de la red, por una parte, y el comportamiento fraudulento de cualquiera de las partes involucradas en el intercambio, por la otra, pueden ocasionar situaciones en las que una de las dos partes proporcione el bien o realice el pago y no reciba, a cambio, el pago o el bien de la otra parte. La atomicidad permite vincular una serie de operaciones de modo que se ejecuten en su totalidad o no se ejecuten en absoluto. El intercambio atómico pretende que el intercambio se realice totalmente o no se realice, y por tanto, no haya pérdidas para ninguna de las dos partes.

La confianza que un usuario deposita en un servicio es fundamental a la hora de decidirse a utilizarlo. La seguridad de que los pagos realizados tienen garantizada la entrega del bien, es decir, la atomicidad, puede representar un aumento en la confianza que la transacción económica inspira al usuario, que de otra manera puede no estar dispuesto a realizar un pago sin la certeza de la recepción del producto.

En la compra de bienes digitales utilizando moneda electrónica, tanto el bien como la moneda se transmiten en línea, ya que el bien se puede ofrecer electrónicamente y, por tanto, las partes pueden intercambiar directamente la moneda electrónica y el bien adquirido, en una operación denominada pago a cambio de un producto. Si la compra es de un bien tangible, y por tanto requiere un envío físico, el intercambio no se formalizará entre bien y moneda, sino que la alternativa es un intercambio de la moneda por un recibo del pago. El recibo consistirá en un compromiso por parte del vendedor donde se refleja la evidencia del pago y la descripción del bien que será transferido a través de un envío físico. Este recibo será utilizado como prueba de la conclusión de la compra en caso de disputa.

Los fallos de la red pueden dar lugar a situaciones en las que las monedas pueden pasar a estar en un estado ambiguo, donde se podría llegar, incluso, a perder su valor. Por ejemplo, en un sistema de moneda electrónica anónima fuera de línea con detección de reutilización en el que un fallo ocasiona que un pagador no pueda saber si el receptor ha recibido o no la moneda, no se puede arriesgar a utilizarla de nuevo, ya que si lo hiciera y el pago se hubiera preparado, el usuario no solo sería identificado, sino que también sería acusado de reutilización.

Ejercicios de autoevaluación

1. Observad el funcionamiento de la fase de pago de varios establecimientos comerciales virtuales. ¿Qué sistemas de pago utilizan? Describidlos.
En el caso de permitir pagos mediante tarjeta de crédito, ¿qué mecanismo de autenticación habéis podido observar?

2. Describid el funcionamiento de un algoritmo concreto de firma ciega.
En general, ¿creéis que sería posible realizar una firma sobre un conjunto de información de la que una parte estuviera visible (y se pudiera verificar) y otra parte estuviera oculta?

3. ¿Es posible hacer un sistema de micropago anónimo?
En caso afirmativo, proponed una técnica para hacerlo o describid alguna propuesta publicada.

Bibliografía

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

Chaum, D.; Fiat, A.; Naor, M. (1988). "Untraceable Electronic Cash" (pág. 319-327). *CRYPTO'88: Proceedings on Advances in Cryptology, LNCS 403*.

Rivest, R. L.; Shamir, A. (1996). *PayWord and MicroMint: two simple micropayment schemes* (pág. 69-87). CryptoBytes.