(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 609 011**

(51) Int. CI.:

G06Q 20/28 (2012.01)
G06Q 20/36 (2012.01)
G06Q 20/34 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **08.02.2013 PCT/EP2013/052594**

(87) Fecha y número de publicación internacional: **15.08.2013 WO13117726**

(96) Fecha de presentación y número de la solicitud europea: **08.02.2013 E 13703104 (3)**

(97) Fecha y número de publicación de la concesión europea: **12.10.2016 EP 2812864**

(54) Título: **Sistema de pago, terminal de pago de este sistema y procedimiento de pago asociado**

(30) Prioridad:

09.02.2012 FR 1200388

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.04.2017

(73) Titular/es:

THALES (100.0%)
45, rue de Villiers
92200 Neuilly-sur-Seine, FR

(72) Inventor/es:

D'ATHIS, THIERRY;
LEONETTI, JEAN y
RATIER, DENIS

(74) Agente/Representante:

SALVA FERRER, Joan

DESCRIPCIÓN

Sistema de pago, terminal de pago de este sistema y procedimiento de pago asociado.

[0001] La presente invención se refiere a un sistema de pago y un soporte de pago electrónico adaptado para dialogar con el terminal de pago, siendo el soporte de pago portador de un importe que tiene un primer valor residual y que comprende:

- una primera memoria regrabable, y
- una segunda memoria de fusibles, que comprende una pluralidad de bits adaptados para cambiar de estado una única vez cada uno.

[0002] En la actualidad, los sistemas de pago que utilizan unos soportes de pago electrónicos se multiplican. Estos sistemas de pago son particularmente ventajosos ya que permiten una automatización de la transacción de pago y, por tanto, una aceleración de esta. Los soportes de pago electrónicos utilizados reagrupan unos objetos tan diferentes como los monederos electrónicos, portadores de una moneda fiduciaria, las tarjetas de pago, que permiten el débito de una cuenta bancaria después de la teletransmisión de una orden de pago y las tarjetas de prepago, distribuidas por ciertos organismos y portadoras de un importe monetario o no monetario (como unas unidades de transporte) electrónico representativo de una suma de dinero depositada por el usuario de la tarjeta en el organismo distribuidor.

[0003] Unos ejemplos de tarjetas de prepago son las tarjetas de comedor, las tarjetas de tienda, las tarjetas de ubicación, las tarjetas de teléfono público o las tarjetas de transporte público.

[0004] Unas tarjetas de prepago deben responder a dos objetivos contradictorios: deben tener por una parte un coste de producción mínimo y, por otra parte, presentar una seguridad suficiente para evitar unas manipulaciones fraudulentas del valor residual del importe monetario guardado en la tarjeta.

[0005] Existen unas tarjetas de prepago que constan de una computación rápida, es decir, un procesador optimizado para las tareas de criptografía, adaptados para bloquear el acceso a la memoria de la tarjeta a unos terminales no autorizados. No obstante, estas tarjetas tienen un coste de fabricación elevado.

[0006] Existen unos soportes de coste reducido, tales como los tickets sin contacto, que constan simplemente de unos medios de comunicación con un terminal, una memoria regrabable y una memoria de fusibles (denominada memoria OTP, para «one time programmable»). En particular, estos soportes de coste reducido no comprenden procesador.

[0007] La tarjeta inteligente descrita en la solicitud FR 2 636 153 es un ejemplo tal de un soporte de coste reducido.

[0008] No obstante, la utilización de estos soportes como tarjetas de prepago es problemática. En efecto, si el importe está escrito en la memoria regrabable del soporte, es fácil para una persona malintencionada estafar reescribiendo el valor residual de este importe; la exigencia de seguridad de la tarjeta de prepago no se cumple entonces. Otra solución es hacer corresponder el valor residual del importe cargado en la tarjeta con los estados de los bits de la memoria de fusibles. Sin embargo, el reducido número de bits de la memoria de fusibles (generalmente unas decenas) impide utilizar esta memoria para valorar un equivalente monetario.

[0009] Un objetivo de la invención es, por tanto, proponer un sistema y un procedimiento de pago que utilizan unos soportes de pago de bajo coste y adaptados para limitar las posibilidades de fraude. Otros objetivos son garantizar la atomicidad y la coherencia de las transacciones de pago.

[0010] A tal efecto, la invención tiene como objeto un sistema de pago del tipo precitado, en el cual el terminal de pago está programado para deducir el primer valor residual de la lectura conjunta de la primera y segunda memorias.

[0011] Según unos modos de realización preferidos de la invención, el sistema de pago presenta una o varias de las características siguientes, tomada(s) aisladamente o según toda(s) la(s) combinación(es) técnicamente posible(s):

- el soporte de pago es un soporte sin contacto, adaptado para dialogar a distancia con el terminal de pago;
- el sistema de pago está programado para aplicar un procedimiento tal como se defina más abajo.

[0012] La invención tiene igualmente como objeto un terminal de pago de un sistema tal como se ha definido más arriba.

[0013] La invención tiene además como objeto un procedimiento de pago por medio de un soporte de pago adaptado para dialogar a distancia con un terminal de pago, siendo el soporte de pago portador de un importe y comprendiendo una primera memoria regrabable y una segunda memoria de fusibles que comprende una pluralidad de bits adaptados para cambiar de estado una única vez cada uno, caracterizado porque comprende las etapas sucesivas siguientes:

- puesta en comunicación del soporte de pago con el terminal de pago, teniendo el importe un primer valor residual
- lectura de la primera y segunda memorias, y
- deducción del primer valor residual a partir de los datos leídos en la primera y segunda memorias.

[0014] Según unos modos de realización preferidos de la invención, el procedimiento de pago presenta una o varias de las características siguientes, tomada(s) aisladamente o según toda(s) la(s) combinación(es) técnicamente posible(s):

- dicho procedimiento de pago comprende las etapas siguientes:

    - asignación al importe de un segundo valor residual, inferior al primer valor residual reemplazando el primer valor residual, y
    - cambio de estado de al menos un bit de la segunda memoria, pasando el o cada bit de un primer estado a un segundo estado, cuando la diferencia entre el primer y segundo valores residuales es superior a un valor umbral.

- el número de bits que cambia de estado va en función de la diferencia entre el primer y segundo valores residuales;
- una imagen del primer valor residual se guarda en la primera memoria y el procedimiento comprende una etapa de escritura en la primera memoria de una imagen del segundo valor residual, reemplazando la imagen del primer valor residual;
- una imagen del primer valor residual está guardada en la primera memoria y el procedimiento comprende además las etapas siguientes:

    - determinación de un intervalo de valores residuales autorizados para el importe, en función de los estados de los bits de la segunda memoria,
    - control de la adecuación entre la imagen del primer valor residual y el intervalo de valores residuales autorizados, y
    - si la imagen del primer valor residual es superior al intervalo de valores residuales autorizados, negativa de pago, o cambio de la imagen del primer valor residual para que esté comprendido en el intervalo de valores residuales autorizados;

- si el primer valor residual es inferior al intervalo de valores residuales autorizados, dicho procedimiento de pago comprende una etapa de cambio de la imagen del primer valor residual para que esté comprendido en el intervalo de valores residuales autorizados;
- el procedimiento comprende igualmente una etapa de escritura de una copia de seguridad del importe en la primera memoria,

el procedimiento es tal que:

- la etapa de cambio de estado del o de cada bit tiene lugar después de la etapa de escritura de la imagen del segundo valor residual,
- una copia de seguridad del importe, que tiene un primer valor de copia de seguridad, se guarda en la primera memoria durante la puesta en comunicación del soporte de pago con el terminal de pago, y porque
- el procedimiento comprende una etapa suplementaria de escritura de un segundo valor de copia de seguridad, igual al segundo valor residual, reemplazando el primer valor de copia de seguridad, siguiendo esta etapa a la etapa de cambio de estado de al menos un bit de la segunda memoria;

- dicho procedimiento de pago comprende además las etapas siguientes:

- determinación de un intervalo de valores residuales autorizados para el importe en función de los estados de los bits de la segunda memoria,
- control de la adecuación de la imagen del primer valor residual y del primer valor de copia de seguridad con el intervalo de valor residual autorizados, y
- si la imagen del primer valor residual está fuera del intervalo de valores residuales autorizados y el primer valor de copia de seguridad está en el intervalo de valores residuales autorizados, cambio de la imagen del primer valor residual para que sea igual al primer valor de copia de seguridad, o
- si la imagen del primer valor residual está en el intervalo de valores residuales autorizados y el primer valor de copia de seguridad está fuera del intervalo de valores residuales autorizados, cambio del primer valor de copia de seguridad para que sea igual a la imagen del primer valor residual.

- la etapa de determinación del intervalo de valores residuales autorizados comprende las etapas siguientes:

- asociación de un intervalo predeterminado de valores a cada bit de la segunda memoria,
- identificación del último bit de la segunda memoria que puede cambiar de estado, y
- determinación del intervalo de valores residuales autorizados como igual al intervalo predeterminado asociado al bit identificado.

- la etapa de determinación del intervalo de valores residuales autorizados comprende las etapas siguientes:

- asociación de un intervalo predeterminado de valores a cada número entero comprendido entre cero y el número de bits,
- recuento del número de bits de la segunda memoria que no ha cambiado de estado, y
- determinación del intervalo de valores residuales autorizados como igual al intervalo predeterminado asociado al número de bits contados.

[0015] Otras características y ventajas de la invención se mostrarán con la lectura de la descripción que aparece a continuación, dada únicamente a título de ejemplo y realizada en referencia a los dibujos anexos, en los cuales:

- la figura 1 es una vista esquemática de un sistema de pago según la invención, cuando un soporte de pago de este sistema no se ha utilizado nunca,
- la figura 2 es una vista similar a la figura 1, cuando un importe que se había cargado en el soporte se ha gastado completamente,
- la figura 3 es un esquema que ilustra un vínculo entre los estados de bits de una memoria de fusibles del soporte y un intervalo de valores residuales autorizados para el importe, según un primer modo de realización de la invención,
- la figura 4 es un esquema que ilustra un vínculo entre los estados de bits de una memoria de fusibles del soporte y un intervalo de valores residuales autorizados para el importe, según un segundo modo de realización de la invención,
- la figura 5 es una vista similar a la figura 1, tras una etapa de cambio de una imagen del valor residual del importe cargado en el soporte,
- la figura 6 es una vista similar a la figura 1, tras una etapa de cambio de estado de varios bits de la memoria de fusibles,
- la figura 7 es una vista similar a la figura 1, tras una etapa de escritura de un valor nuevo de copia de seguridad del importe en una memoria regrabable del soporte,
- la figura 8 es un diagrama de bloques que ilustra un procedimiento según la invención.

[0016] El sistema 10 de pago según la invención, representado en la figura 1, comprende un terminal de pago 12 y un soporte de pago sin contacto 14, adaptado para dialogar a distancia con el terminal de pago 12 para realizar una transacción de pago.

[0017] De forma conocida, el terminal de pago 12 comprende una antena 20, un módulo radio 22 según la norma ISO 14443, adaptado para gestionar los intercambios de datos a distancia entre el terminal 12 y el soporte 14, y un módulo 24 de gestión de la transacción de pago entre el terminal 12 y el soporte 14.

[0018] El soporte de pago 14 comprende una antena 30, un módulo radio 32 según la norma ISO 14443, adaptado para gestionar los intercambios de datos a distancia entre el terminal 12 y el soporte 14, una primera memoria 34 regrabable, una segunda memoria 36 de fusibles y un enlace serie 38 que pone en comunicación el módulo radio 32 con las memorias 34, 36. En particular, el soporte de pago 14 no comprende computación rápida.

[0019] El soporte de pago 14 es portador de un importe, con un primer valor residual. El importe está dividido en unidades, divididas en sí en subdivisiones; por ejemplo, en el caso de un importe monetario en euros, las unidades son los euros y las subdivisiones son los céntimos de euros. El primer valor residual se formula en número de unidades y de subdivisiones.

[0020] El importe es, de preferencia, un importe monetario. Corresponde a una suma de dinero depositada por el usuario del soporte 14 a un distribuidor del soporte 14 para adquirir el soporte 14. El valor residual es igual al valor inicial del importe, al cual se han retirado los gastos eventuales ya efectuados por el usuario del soporte 14 por medio del soporte 14.

[0021] El soporte de pago 14 no es recargable, es decir que, una vez que el importe se ha gastado íntegramente, ya no es posible utilizar el soporte de pago 14.

[0022] La memoria de fusibles 36 comprende una pluralidad de bits 1, 2, 3, 4, 5, 6, 7, 8, estando cada bit 1, 2, 3, 4, 5, 6, 7, 8 adaptado para estar selectivamente en un primer o un segundo estado y para cambiar de estado una única vez. En particular, cada bit 1, 2, 3, 4, 5, 6, 7, 8 está autorizado a cambiar del primer estado al segundo estado, pero le es imposible volver del segundo estado al primer estado.

[0023] En el ejemplo representado en la figura 1, todos los bits 1, 2, 3, 4, 5, 6, 7, 8 están en el primer estado. Esto corresponde a la configuración del soporte 14 durante su adquisición por su usuario. En el ejemplo representado en la figura 2, todos los bits 1, 2, 3, 4, 5, 6, 7, 8 están en el segundo estado. Esto corresponde a la configuración del soporte 14 cuando se ha gastado la totalidad del importe.

[0024] El módulo de gestión 24 está programado para deducir el primer valor residual del importe de la lectura conjunta de la primera y segunda memorias 34, 36. En particular, por «lectura conjunta», se comprende que es necesario para el módulo de gestión 24 leer estas dos memorias 34, 36 para deducir el primer valor residual, no siendo suficiente la lectura de una sola de estas memorias 34, 36 para la deducción del primer valor residual. Este punto se detallará a continuación.

[0025] El módulo de gestión 24 está programado igualmente para:

- calcular un segundo valor residual del importe, igual a la diferencia entre el primer valor residual y el precio de una compra regulada durante la transacción de pago,
- asignar el segundo valor residual al importe, reemplazando el primer valor residual, y
- controlar el cambio de estado de al menos un bit 6, 7, 8 de la segunda memoria 36, del primer estado en el segundo estado, cuando la diferencia entre el primer y segundo valores residuales es superior a un valor umbral.

[0026] En un primer modo de realización de la invención, ilustrado por las figuras de 1 a 8, una imagen V_1 del primer valor residual se guarda en la primera memoria 34. Siempre que la última transacción de pago en la cual está implicado el soporte 14 se desarrolle correctamente, esta imagen V_1 será igual al primer valor residual.

[0027] Una copia de seguridad M' del importe se guarda igualmente en la primera memoria 34. Esta copia de seguridad M' tiene un primer valor de copia de seguridad V_1. Siempre que la última transacción de pago en la cual se ha implicado el soporte 14 se desarrolle correctamente, el primer valor de copia de seguridad V_1' será igual al primer valor residual.

[0028] En referencia a las figuras 3 y 4, el módulo de gestión 24 se programa para determinar un intervalo T de valores residuales autorizados para el importe en función de los estados de los bits 1, 2, 3, 4, 5, 6, 7, 8 de la segunda memoria 36. Así, un usuario malintencionado que intentaría cambiar fraudulentamente la imagen del primer valor residual V_1 para aumentar el valor no podría ir más allá del intervalo de valores residuales autorizados T sin que esto sea detectado por el terminal de pago 12. Los riesgos de fraude se reducen de este modo.

[0029] A tal efecto, en una primera variante de la invención, ilustrada por la figura 3, el módulo de gestión 24 asocia un intervalo predeterminado T_0, ..., T_i, ..., T_8 de valores a cada número entero i comprendido entre cero y el número de bits 1, 2, 3, 4, 5, 6, 7, 8. Cada intervalo predeterminado, respectivamente T_0, ..., T_i, ..., T_8, está limitado por un borne inferior, respectivamente B_0, ..., B_i, ... B_8, y por un borne superior, respectivamente B_1, ..., B_{i+1}, ... B_9. El borne más pequeño inferior B_0 es el valor 0 y el borne mayor superior B_9 es el valor inicial del importe.

[0030] De preferencia, el borne B_1 es el valor más pequeño inmediatamente superior a 0. Así, el intervalo predeterminado T_0 se limita al valor 0.

[0031] El número de gestión 24 está adaptado para, en cada transacción de pago, contar los bits 1, 2, 3, 4, 5, 6, 7, 8 de la segunda memoria 36 que están en el primer estado y para determinar el intervalo T de valor residual autorizado como igual al intervalo predeterminado T_0, ..., T_i, ..., T_8 asociado al número de bits contados. En el ejemplo representado en la figura 3, el número de bits 1, 2, 3, 4, 5 que están en el primer estado siendo igual a cinco, el módulo de gestión 24 determina que el intervalo T de valores residuales autorizados es el intervalo predeterminado T_5.

[0032] En una segunda variante preferida de la invención, ilustrada por la figura 4, cada intervalo predeterminado T_0, ..., T_i, ..., T_8 está asociado no a un número entero i, sino a un bit i-1 particular. A tal efecto, el módulo de gestión 24 está adaptado para identificar cada bit 1, 2, 3, 4, 5, 6, 7, 8 de la segunda memoria 36 de manera específica. Un medio de realizar tal identificación específica es conocido por el experto en la técnica y no se describirá aquí.

[0033] El módulo de gestión 24 está programado igualmente para identificar el último bit 1, 2, 3, 4, 5, 6, 7, 8 que ha cambiado de estado. Esto se realiza por ejemplo confiriendo un orden particular a los bits 1, 2, 3, 4, 5, 6, 7, 8 de la segunda memoria 36, cambiando los bits 1, 2, 3, 4, 5, 6, 7, 8 de estado según este orden particular. El último bit 1, 2, 3, 4, 5, 6, 7, 8 que ha cambiado de estado es así fácilmente identificable como el bit en el segundo estado más avanzado en el orden de cambio de estado. En el ejemplo representado, los bits 1, 2, 3, 4, 5, 6, 7, 8 que cambian de estado según el orden inverso de su numeración y el último bit que ha cambiado de estado es el bit 6.

[0034] El módulo de gestión 24 está programado por último para determinar el intervalo T de valores residuales autorizados como igual al intervalo predeterminado T_0, ..., T_i, ..., T_8 asociado al último bit que ha cambiado de estado. En el ejemplo representado, el intervalo T es así igual al intervalo predeterminado asociado al bit 6, a saber T_7.

[0035] Se observará que es posible, especialmente durante la primera utilización del soporte 14, que ningún bit haya cambiado aún de estado. El intervalo predeterminado T_8 está asociado a este caso.

[0036] El módulo de gestión 24 está programado además para efectuar las operaciones sucesivas siguientes, durante una transacción de pago por medio del soporte 14 durante la cual el usuario del soporte 14 regula una compra a un precio dado:

- determinar el intervalo T de valores residuales autorizados para el importe,
- controlar la adecuación de la imagen del primer valor residual V_1 y del primer valor de copia de seguridad V_1' con el intervalo T de valores residuales autorizados, es decir controlar que la imagen del primer valor residual V_1 y el primer valor de copia de seguridad V_1' estén comprendidos en el intervalo T, y
    - ○ rechazar el pago y poner fin a la transacción de pago si la imagen del primer valor residual V_1 es superior al intervalo T o cambiar la imagen del primer valor residual V_1 para que sea igual al primer valor de copia de seguridad V_1', si la imagen del primer valor residual V_1 está fuera del intervalo T y el valor de copia de seguridad V_1' está en el intervalo T, o
    - ○ cambiar el primer valor de copia de seguridad V_1' para que sea igual a la imagen del valor residual V_1', si la imagen del primer valor residual V_1 está en el intervalo T y el valor residual de copia de seguridad V_1' está fuera del intervalo T, o
    - ○ cambiar la imagen del primer valor residual V_1 para que sea igual al borne inferior del intervalo T y cambiar el primer valor de copia de seguridad V_1' para que sea igual al primer valor residual nuevo, si la imagen del primer valor residual V_1 y e primer valor de copia de seguridad V_1' están ambos fuera del intervalo T, o
    - ○ dejar la imagen del primer valor residual V_1 y el primer valor de copia de seguridad V_1' sin cambios, si están ambos en el intervalo T,

- autorizar el pago,
- reemplazar la imagen del primer valor residual V_1 por una imagen del segundo valor residual V_2 (Figura 5),
- si el segundo valor residual V_2 no está en el intervalo T de valores residuales autorizados, en otros términos si el precio es superior a un valor umbral de cambio de intervalo, igual a la diferencia entre el primer valor V_1 y el borne inferior B_5 del intervalo T, controlar el cambio de estado de al menos un bit 6, 7, 8 de la segunda memoria 36 del primer estado hacia el segundo estado (véase la figura 6), dependiendo el número de bits 6, 7, 8 que cambia de

estado de la diferencia entre el primer y segundo valor residuales V_1, V_2,
- validar el pago,
- reemplazar el primer valor de copia de seguridad V_1' por un segundo valor de copia de seguridad V_2' (figura 7) igual al segundo valor residual V_2, y
- poner fin a la transacción de pago.

[0037] Un procedimiento de pago por medio del sistema de pago 10 se va a describir ahora, con respecto a la figura 8. Este procedimiento se produce cuando el usuario del soporte 14 desea regular una compra a un precio dado.

[0038] Durante una primera etapa 100, el terminal 12 y el soporte 14 se ponen en comunicación uno con otro. Esta operación se realiza característicamente colocando el soporte 14 a una distancia suficiente del terminal 12 para permitir el acoplamiento electromagnético de las antenas 20, 30 del terminal 12 y del soporte 14.

[0039] Después, durante una primera etapa 102, el módulo de gestión 24 lee la primera y segunda memoria 34, 36. En particular, el terminal 12 recupera la información guardada en la primera memoria 34, y:

- en la primera variante de la invención, recuenta los bits 1, 2, 3, 4, 5, 6, 7, 8 de la segunda memoria 36 que están en el primer estado, o
- en la segunda variante de la invención, identifica el último bit de la segunda memoria 36 que debe haber cambiado de estado

[0040] Esta primera etapa 102 está seguida de una segunda etapa 104 de deducción del primer valor residual.

[0041] La segunda etapa 104 comprende una primera subetapas 105 de determinación del intervalo T de valores residuales autorizados, durante la cual:

- en la primera variante de la invención, el módulo de gestión 24 determina el intervalo T como igual al intervalo predeterminado T_8 asociado al número de bits 1, 2, 3, 4, 5, 6, 7, 8 contados como que están en el primer estado, o
- en la segunda variante de la invención, el módulo de gestión 24 determina el intervalo T como que es igual al intervalo predeterminado T_8 asociado al último bit de la memoria 36 que ha cambiado de estado.

[0042] La etapa 105 está seguida por una etapa 110 de control de la adecuación de la imagen del primer valor residual V_1 con el intervalo T de valores residuales autorizados. Durante esta etapa 110, el módulo de gestión 24 verifica que la imagen del primer valor residual V_1 está comprendida en el intervalo T. Si la imagen del primer valor residual V_1 está en el intervalo T, el procedimiento pasa a una etapa 120; en el caso contrario, el procedimiento pasa a otra etapa 130.

[0043] Las etapas 120 y 130 son unas etapas de control de la adecuación del primer valor de copia de seguridad residual V_1' con el intervalo T de valores residuales autorizados. Durante estas etapas 120, 130, el módulo de gestión 24 verifica que el primer valor de copia de seguridad V_1' está comprendido en el intervalo T.

[0044] Si durante la etapa 120, el primer valor de copia de seguridad V_1' está en el intervalo T, el procedimiento pasa a una etapa 140; en el caso contrario, el procedimiento pasa a otra etapa 150.

[0045] Si durante la etapa 130, el primer valor de copia de seguridad V_1' está en el intervalo T, el procedimiento pasa a una etapa 160; en el caso contrario, el procedimiento pasa a otra etapa 170.

[0046] La etapa 140 es una etapa de autorización de pago. Durante esta etapa, el módulo de gestión 24 deduce que el primer valor residual es igual a la imagen del primer valor residual V_1 guardado en la primera memoria 34. El módulo de gestión 24 considera entonces que las condiciones necesarias para la realización efectiva del pago se cumplen y lo notifica a los otros módulos (no representados) del terminal de pago 12 igualmente implicados en la transacción, por ejemplo a un módulo de visualización.

[0047] La etapa 150 es una etapa de puesta en conformidad del primer valor de copia de seguridad V_1' con la imagen del primer valor residual V_1. Durante esta etapa, el primer valor de copia de seguridad V_1' se cambia para que sea igual a la imagen del primer valor residual V_1. En otros términos, el primer valor de copia de seguridad V_1' se reescribe, siendo el primer valor de copia de seguridad nuevo V_1' igual a la imagen del primer valor residual V_1. La

etapa 150 está seguida por la etapa 140.

[0048] La etapa 160 es una etapa de puesta en conformidad de la imagen del primer valor residual V_1 con el primer valor de copia de seguridad V_1'. Durante esta etapa, la imagen del primer valor residual V_1 se cambia para que sea igual al primer valor de copia de seguridad V_1'. En otros términos, la imagen del primer valor residual V_1 se reescribe, siendo la nueva imagen del primer valor residual V_1 igual al valor de copia de seguridad V_1'. La etapa 160 está seguida por la etapa 140.

[0049] La etapa 170 es una nueva etapa de control de la adecuación de la imagen del primer valor residual V_1 con el intervalo T de valores residuales autorizados. Durante esta etapa, el módulo de gestión 24 controla si la imagen del primer valor residual V_1 es inferior al intervalo T. Si la imagen del primer valor residual V_1 es efectivamente inferior al intervalo T, el procedimiento pasa a una etapa 180; en el caso contrario, el procedimiento pasa a una etapa 190.

[0050] La etapa 180 es una etapa de puesta en conformidad de la imagen del primer valor residual V_1 y del primer valor de copia de seguridad V_1'. Durante esta etapa 180, la imagen del primer valor residual V_1 y el primer valor de copia de seguridad V_1' se cambian para que sean iguales al borne inferior del intervalo T. En otros términos, la imagen del primer valor residual V_1 y el primer valor de copia de seguridad V_1' se reescriben, siendo la nueva imagen del primer valor residual V_1 y primer valor de copia de seguridad V_1' iguales al borne inferior del intervalo T. Como variante, la nueva imagen del primer valor residual V_1 y primer valor de copia de seguridad V_1' son iguales a otro valor del intervalo T. La etapa 180 está seguida por la etapa 140.

[0051] La etapa 190 es una etapa de negativa de pago. Durante esta etapa, el módulo de gestión 24 constata el fracaso de la deducción del primer valor residual del importe y deduce que el soporte 14 ha sido falsificado. Lo rechaza como medio de pago y lo notifica a los otros módulos del terminal de pago 12 igualmente implicados en la transacción. La etapa 190 está seguida por una etapa 200 de parada de la transacción.

[0052] Las etapas 110, 120, 130, 140, 150 160, 170, 180, 190 son unas subetapas de la segunda etapa 104.

[0053] A la segunda etapa 104 la sucede una tercera etapa 202 de cambio del valor residual del importe. Durante esta etapa 202, el módulo de gestión 24 interviene en las memorias 34, 36 del soporte 14 para asignar al importe un segundo valor residual, inferior al primer valor residual, reemplazando el primer valor residual. En particular, el segundo valor residual es igual a la diferencia entre el primer valor residual y el precio de la compra.

[0054] La tercera etapa 202 sucede más particularmente a la etapa 140.

[0055] La tercera etapa 202 comprende una primera subetapas 210 de cambio de la imagen del valor residual del importe. Durante esta subetapas 210, el módulo de gestión 24 reemplaza la imagen del primer valor residual V_1 por una imagen del segundo valor residual V_2, igual al segundo valor residual.

[0056] La subetapas 210 está seguida por una etapa 212 de control de la pertenencia del segundo valor residual al intervalo T de valores autorizados. Si el segundo valor residual no pertenece al intervalo T, la etapa 212 está seguida de una etapa 220 de cambio de estado de al menos un bit 6, 7, 8 de la segunda memoria 36, del primer estado hacia el segundo estado. Si el segundo valor residual pertenece al intervalo T, la etapa 212 está seguida directamente de una etapa 230 de validación del pago.

[0057] El número de bits 6, 7, 8 que cambia de estado durante la etapa 220 va en función de la diferencia entre el primer y el segundo valor residual. El número de bits 6, 7, 8 que cambia de estado es tal que el segundo valor residual está comprendido en el intervalo predeterminado T_0, ..., T_i, ..., T_8 asociado al número de bits 1, 2, 3, 4, 5 restante en el primer estado tras el cambio de estado de los bits 6, 7, 8 (o asociado al último bit 6 que ha cambiado de estado tras el cambio de estado de dichos bits 6, 7, 8). La etapa 220 está seguida de la etapa 230.

[0058] Durante la etapa 230, el módulo de gestión 24 notifica a los otros módulos del terminal 12 igualmente implicados en la transacción que el pago se ha realizado correctamente. Una vez que se ha realizado esta etapa, el usuario del soporte 14 es libre de disfrutar de su compra.

[0059] Una última etapa 240 de cambio del valor de la copia de seguridad M' sucede a la etapa 230. Durante esta etapa, el módulo de gestión 24 reemplaza el primer valor de copia de seguridad V_1' por un segundo valor de copia de seguridad V_2', igual al segundo valor residual. La etapa 240 está seguida por la etapa 200 de parada de la

transacción.

[0060] Las etapas 212, 220, 230, 240 son unas subetapas de la tercera etapa 202.

[0061] Durante la etapa 200, los intercambios de datos entre el terminal 12 y el soporte 14 se detienen. El módulo de gestión 24 lo notifica al módulo de visualización, que indica que el soporte 14 puede estar alejado del terminal 12.

[0062] Gracias a la invención, los riesgos de fraude se reducen. En efecto, un usuario malintencionado solo podría engañar al sistema 10 modificando la imagen del valor residual en el interior del intervalo T de valores residuales autorizados. Es suficiente con escoger unos bornes intermedios B_1, ..., B_8 entre los intervalos predeterminados T_1, ..., T_8 a unos valores apropiados para que el fraude no sea suficientemente rentable para el usuario para que sea incitado a cometerlo.

[0063] Además, el soporte 14 es poco costoso de producir.

[0064] Por último, la atomicidad y la coherencia de la transacción de pago se garantizan. En efecto, en caso de interrupción brusca e imprevista de la transacción, la presencia del valor de copia de seguridad V_1', V_2' y el orden de las etapas del procedimiento de pago permiten restablecer la coherencia de los datos guardados en el soporte 14.

[0065] Se observará que, en el ejemplo dado más arriba, el soporte de pago 14 no se puede volver a utilizar si la imagen del primer valor residual V_1 es superior al intervalo T de valores residuales autorizados. Como variante, en vez de estar programado para rechazar el pago si la imagen del primer valor residual V_1 es superior al intervalo T de valores residuales autorizados, el módulo de gestión 24 está programado para cambiar la imagen del primer valor residual V_1 de forma que sea igual al borne inferior del intervalo T de valores residuales autorizados.

[0066] En un segundo modo de realización de la invención, no ilustrado, el primer valor residual dividido en un primer valor residual principal y un primer valor residual secundario. De manera ventajosa, el valor residual principal está formulado en número entero de unidades del importe y el valor residual secundario está formulado en número entero de subdivisiones del importe. En el caso de un importe monetario en euros, el valor residual principal es así igual a un número entero de euros y el valor residual secundario es igual a un número entero de céntimos de euros.

[0067] Por ejemplo, el valor residual principal es igual al redondeo por truncamiento del primer valor residual a la unidad inferior y el valor residual secundario es igual a la diferencia entre el primer valor residual y el valor residual principal; el primer valor residual se reconstruye entonces por adición de los valores residuales principal y secundario. Como variante, el valor residual principal es igual al redondeo del primer valor residual a la unidad superior y el valor residual secundario es igual a la diferencia entre el valor residual principal y el primer valor residual; el primer valor residual es entonces igual a la diferencia entre los valores residuales principal y secundario.

[0068] Una imagen del valor residual principal se guarda en la segunda memoria 36 y una imagen del valor residual secundario se guarda en la primera memoria 34.

[0069] El valor residual principal es característicamente igual al número de bits 1, 2, 3, 4, 5, 6, 7, 8 que están en el primer estado.

[0070] La imagen del valor residual secundario es característicamente un número entero comprendido entre 0 y n, donde n es el número de subdivisiones de cada unidad del importe. Por ejemplo, en el caso de un importe monetario, n es igual a 99.

[0071] El módulo de gestión 24 está programado para deducir el primer valor residual del importe de las imágenes de los valores residuales principal y secundario. Característicamente, el módulo de gestión 24 está programado para:

- contar el número de bits 1, 2, 3, 4, 5, 6, 7, 8 de la segunda memoria 36 que están en el primer estado y deducir que el valor residual principal es igual al número de bits recontados,
- deducir el valor residual secundario como igual a la imagen del valor residual secundario, multiplicado por 1/(n+1), y

- deducir el primer valor residual como igual a la suma (como variante la diferencia) de los valores residuales principales y secundarios.

[0072] El módulo de gestión 24 está programado igualmente para anular la transacción si la imagen del valor residual secundario es estrictamente superior a n. Como variante, el módulo de gestión 24 está programado para deducir un valor nulo del valor residual secundario si la imagen del valor residual secundario es estrictamente superior a n.

[0073] Como se ha mencionado más arriba, el módulo de gestión 24 está programado además para asignar un segundo valor residual al importe, reemplazando el primer valor residual, cuando un pago se efectúa por medio del soporte 14. A tal efecto, el módulo de gestión 24 está programado para:

- subdividir el segundo valor residual en un segundo valor residual principal y un segundo valor residual secundario,
- si el segundo valor residual principal es diferente del primer valor residual principal, controlar el cambio de estado de al menos un bit 1, 2, 3, 4, 5, 6, 7, 8 de la segunda memoria 36, de forma que el número de bits restante en el primer estado tras este cambio de estado sea igual al segundo valor residual principal, y
- escribir en la primera memoria 34 una imagen del segundo valor residual secundario, reemplazando la imagen del primer valor residual secundario.

[0074] En este modo de realización, la seguridad del soporte 14 se preserva. En efecto, debido a la irreversibilidad de los cambios aportados a los bits , 2, 3, 4, 5, 6, 7, 8 un usuario malintencionado no podría modificar el valor residual principal del importe, salvo reducirlo, lo que sería contraproducente.

[0075] El módulo de gestión 24 no tiene que efectuar además controles cruzados entre la primera y la segunda memorias 34, 36 para controlar la validez de los datos de la primera memoria 34, contrariamente al primer modo de realización. La transacción es así más rápida.

[0076] Se observará que, en los modos de realización dados más arriba, la segunda memoria 36 solo comprende ocho bits 1, 2, 3, 4, 5, 6, 7, 8. Este dato no es nulamente limitativo y el número de bits de la segunda memoria 36 puede ser cualquiera. Con más frecuencia, la segunda memoria 36 comprenderá treinta y dos bits.

REIVINDICACIONES

1. Procedimiento de pago por medio de un soporte de pago (14) adaptado para dialogar a distancia con un terminal de pago (12), siendo el soporte de pago (14) portador de un importe y comprendiendo una primera memoria (34) regrabable y una segunda memoria (36) de fusibles, que comprende una pluralidad de bits (1, 2, 3, 4, 5, 6, 7, 8) adaptados para cambiar de estado una única vez cada uno, **caracterizado porque** comprende las etapas sucesivas siguientes:

- puesta en comunicación (100) del soporte de pago (14) con el terminal de pago (12), teniendo el importe un valor antes del pago y estando grabada una imagen (V1) del valor antes del pago en la primera memoria (34),
- lectura de la primera y segunda memorias (34, 36), y
- deducción (104) del valor antes del pago a partir de los datos leídos en la primera y segunda memorias (34, 36),

y las etapas siguientes:

- asignación (210) al importe de un valor después del pago, inferior al valor antes del pago, reemplazando el valor antes del pago, y
- cambio de estado (220) de al menos un bit (6, 7, 8) de la segunda memoria (36), pasando el o cada bit (6, 7, 8) de un primer estado a un segundo estado, cuando la diferencia entre los valores anteriores y posteriores al pago es superior a un valor umbral, conllevando el cambio de estado el cambio de un intervalo de valores autorizados para el importe.

comprendiendo la etapa de deducción (104) las subetapas siguientes:

- determinación (105) del intervalo (T) de valores autorizados para el importe en función de los estados de los bits (1, 2, 3, 4, 5, 6, 7, 8) de la segunda memoria (36),
- control (110, 170) de la adecuación entre la imagen del valor antes del pago (V1) y del intervalo de valores autorizados (T), y
- si la imagen del valor antes del pago (V1) es superior al intervalo de valor autorizado (T), negativa de pago (190) o cambio de la imagen del valor antes de pago (V1) para que esté comprendido en el intervalo de valores autorizados (T).

2. Procedimiento de pago según la reivindicación 1, **caracterizado porque** el número de bits (6, 7, 8) que cambia de estado varía en función de la diferencia entre los valores anterior y posterior al pago.

3. Procedimiento de pago según la reivindicación 1 o 2, **caracterizado porque** una imagen (V1) del valor antes del pago está guardada en la primera memoria (34) y **porque** el procedimiento comprende una etapa (210) de escritura en la primera memoria (34) de una imagen (V2) del valor después del pago, reemplazando la imagen del valor antes del pago (V1).

4. Procedimiento de pago según cualquiera de las reivindicaciones anteriores, **caracterizado porque**, si el valor antes del pago (V1) es inferior al intervalo de valores autorizados (T), la etapa de deducción (104) comprende una subetapas (160, 180) de cambio de la imagen del valor antes del pago (V1) para que esté comprendido en el intervalo de valores autorizados (T).

5. Procedimiento de pago según cualquiera de las reivindicaciones anteriores, **caracterizado porque** la etapa (105) de determinación del intervalo de valores autorizados (T) comprende las etapas siguientes:

- asociación de un intervalo predeterminado (T_0, ..., T_i, ..., T_8) de valores a cada bit (1, 2, 3, 4, 5, 6, 7, 8) de la segunda memoria (36),
- identificación del último bit (6) de la segunda memoria (36) que puede cambiar de estado, y
- determinación del intervalo de valores autorizados (T) como igual al intervalo predeterminado (T_0, ..., T_i, ..., T_8) asociado al bit (6) identificado.

6. Procedimiento de pago según cualquiera de las reivindicaciones anteriores, **caracterizado porque** la etapa (105) de determinación del intervalo de valores autorizados (T) comprende las etapas siguientes:

- asociación de un intervalo predeterminado (T_0, ..., T_i, ..., T_8) de valores a cada número entero comprendido entre cero y el número de bits (1, 2, 3, 4, 5, 6, 7, 8),

- recuento del número de bits (1, 2, 3, 4, 5) de la segunda memoria (36) que no ha cambiado de estado, y
- determinación del intervalo de valores autorizados (T) como igual al intervalo predeterminado (T_0, ..., T_i, ..., T_8) asociado al número de bits contados.

7. Sistema de pago (10) que comprende un terminal de pago (12) y un soporte de pago electrónico (14) adaptado para dialogar con el terminal de pago (12), siendo el soporte de pago (14) portador de un importe que tiene un valor antes del pago, y que comprende:

- una primera memoria (34) regrabable, una imagen (V1) del valor antes del pago que se guarda en dicha primera memoria (34), y
- una segunda memoria (36) de fusibles, que comprende una pluralidad de bits (1, 2, 3, 4, 5, 6, 7, 8) adaptados para cambiar de estado una única vez cada uno, **caracterizado porque** el terminal de pago (12) está programado para:
  - deducir el valor antes del pago de la lectura conjunta de la primera y segunda memorias (34, 36),
  - determinar un intervalo (T) de valores autorizados para el importe, en función de los estados de los bits (1, 2, 3, 4, 5, 6, 7, 8) de la segunda memoria (36),
  - controlar la adecuación entre la imagen del valor antes del pago (V1) y el intervalo de valores autorizados (T), rechazar el pago (190) o cambiar la imagen del valor antes del pago (V1) para que esté comprendido en el intervalo de valores autorizados (T), si la imagen del valor antes del pago (V1) es superior al intervalo de valores autorizados (T),
  - asignar al importe un valor después del pago, inferior al valor antes del pago, reemplazando el valor antes del pago, y
  - controlar el cambio de estado de al menos un bit (6, 7, 8) de la segunda memoria (36) cuando la diferencia entre los valores anterior y posterior al pago es superior a un valor umbral, conllevando el cambio de estado un cambio del intervalo de valores autorizados

8. Sistema de pago (10) según la reivindicación 7, **caracterizado porque** el soporte de pago (14) es un soporte sin contacto, adaptado para dialogar a distancia con el terminal de pago (12).

9. Sistema de pago (10) según la reivindicación 7 u 8, **caracterizado porque** el terminal de pago (12) está programado para aplicar un procedimiento según cualquiera de las reivindicaciones de 1 a 6.

10. Terminal de pago (12) de un sistema de pago (10) según cualquiera de las reivindicaciones de 7 a 9.

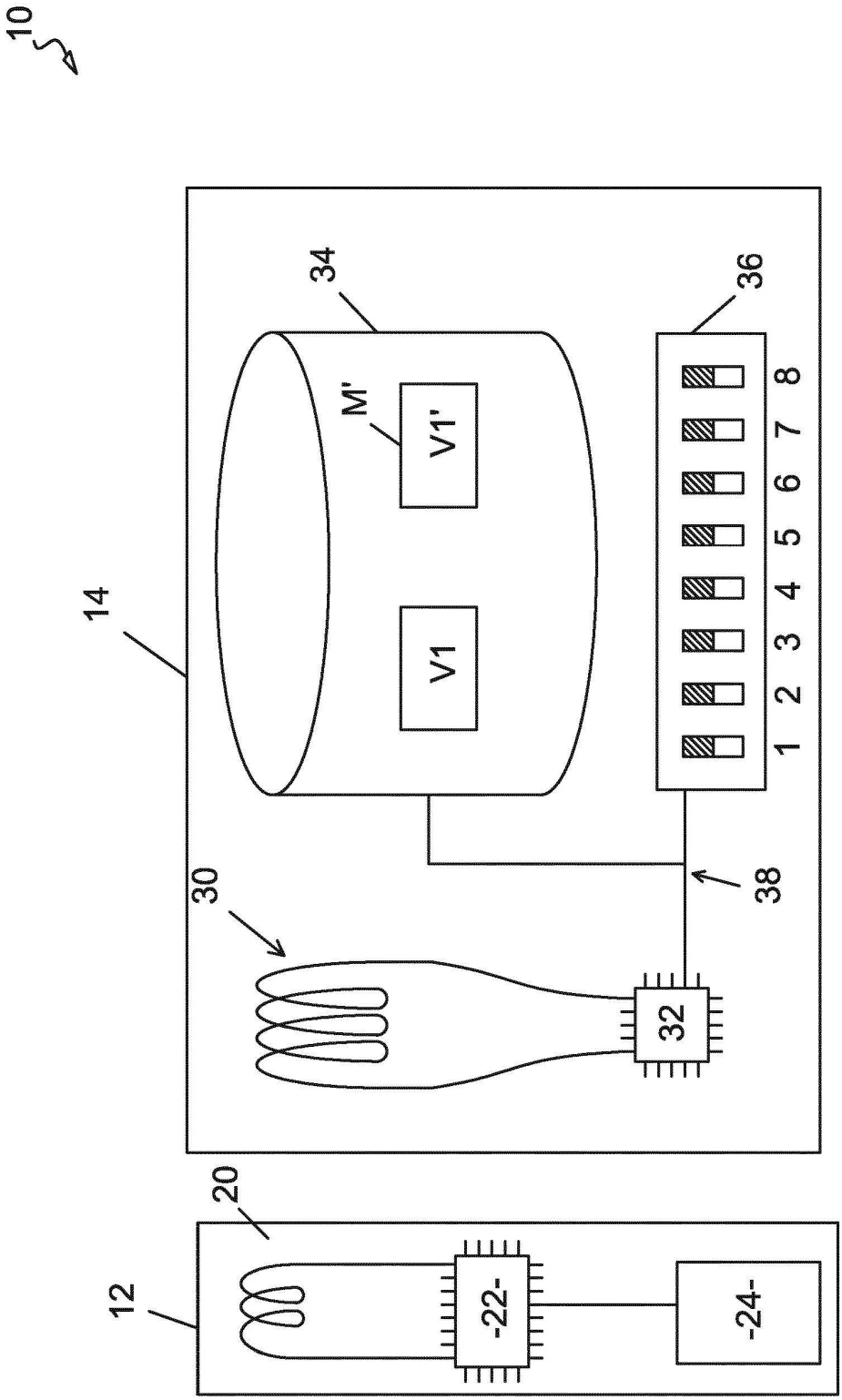

FIG.1

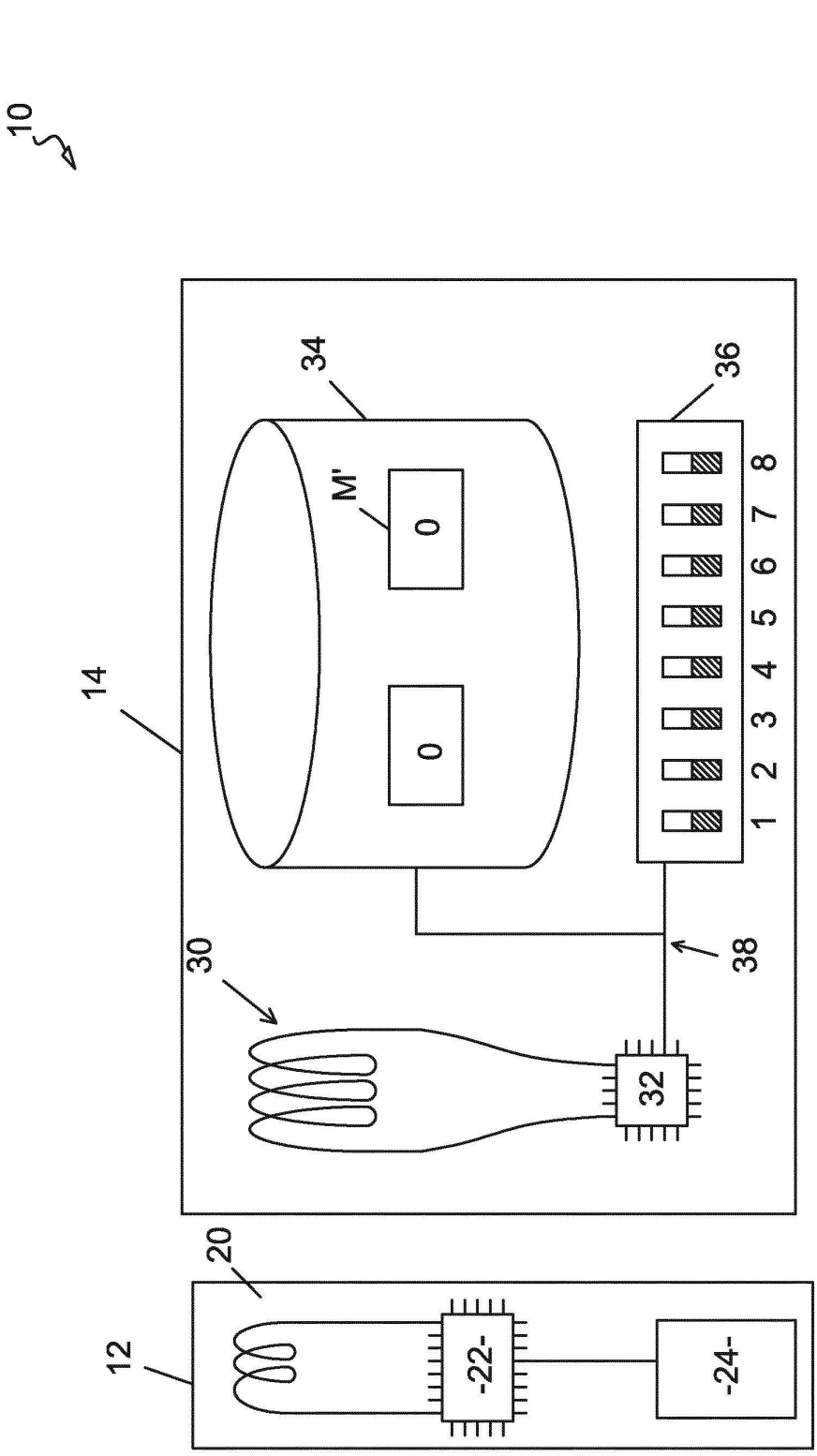

FIG.2

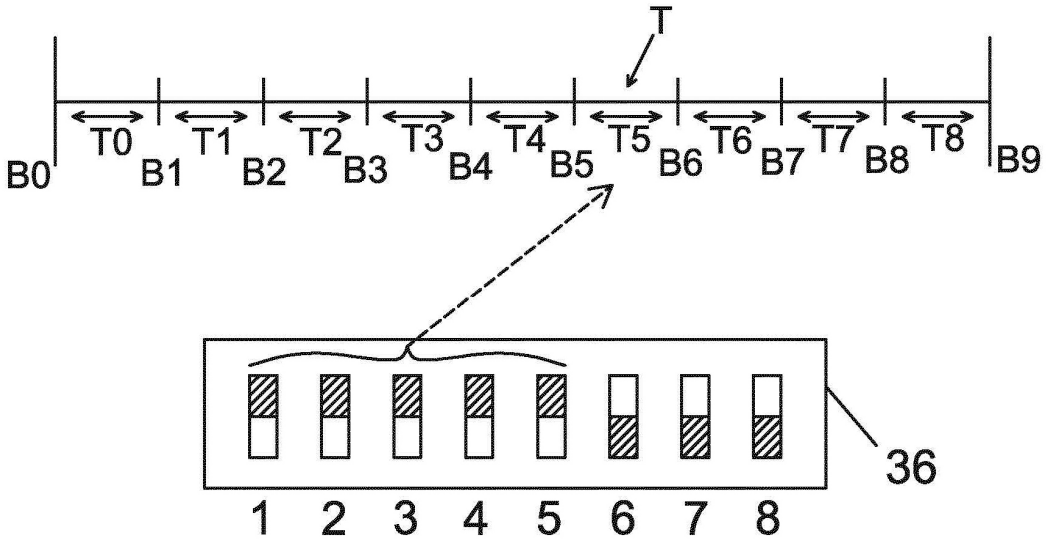
T
T0
T1
T2
T3
T4
T5
T6
T7
T8
B0
B1
B2
B3
B4
B5
B6
B7
B8
B9
36
1
2
3
4
5
6
7
8

FIG.3

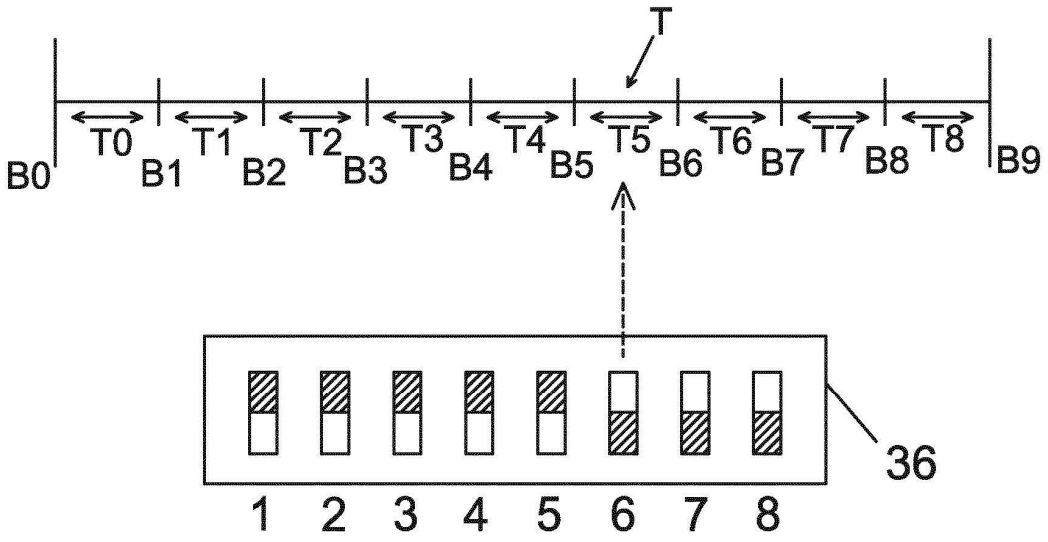
T
T0
T1
T2
T3
T4
T5
T6
T7
T8
B0
B1
B2
B3
B4
B5
B6
B7
B8
B9
36
1
2
3
4
5
6
7
8

FIG.4

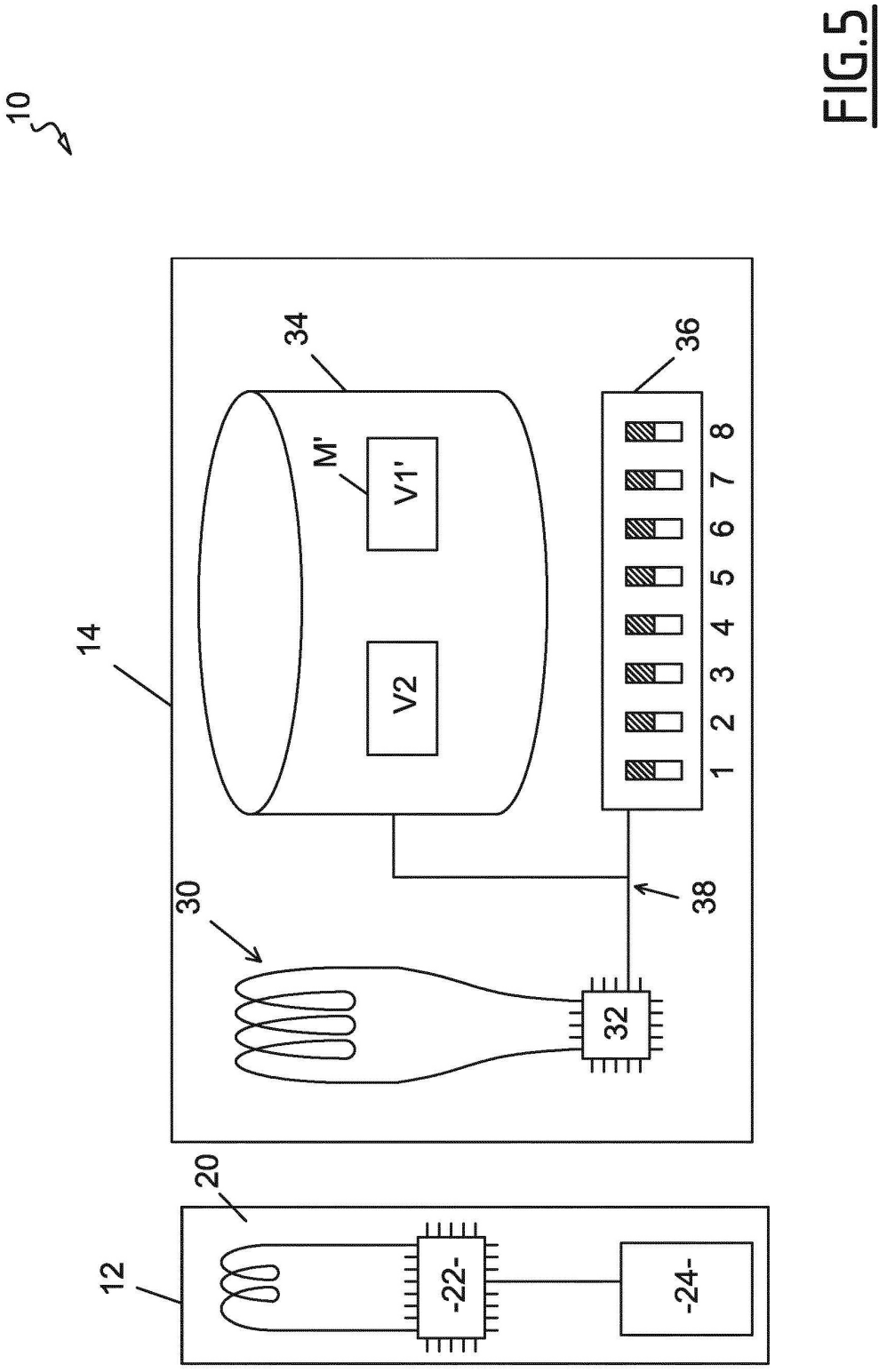

FIG.5

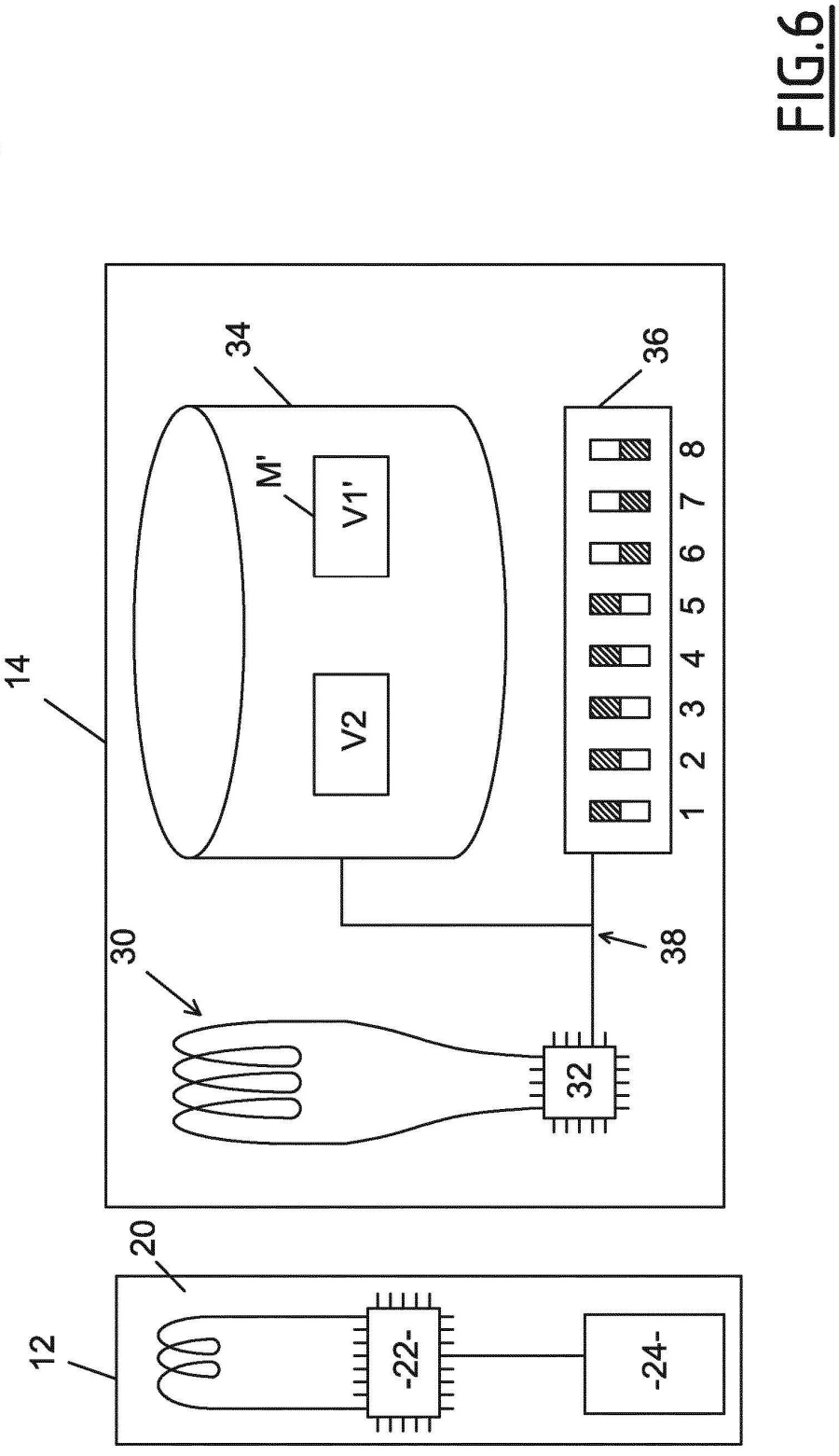

FIG.6

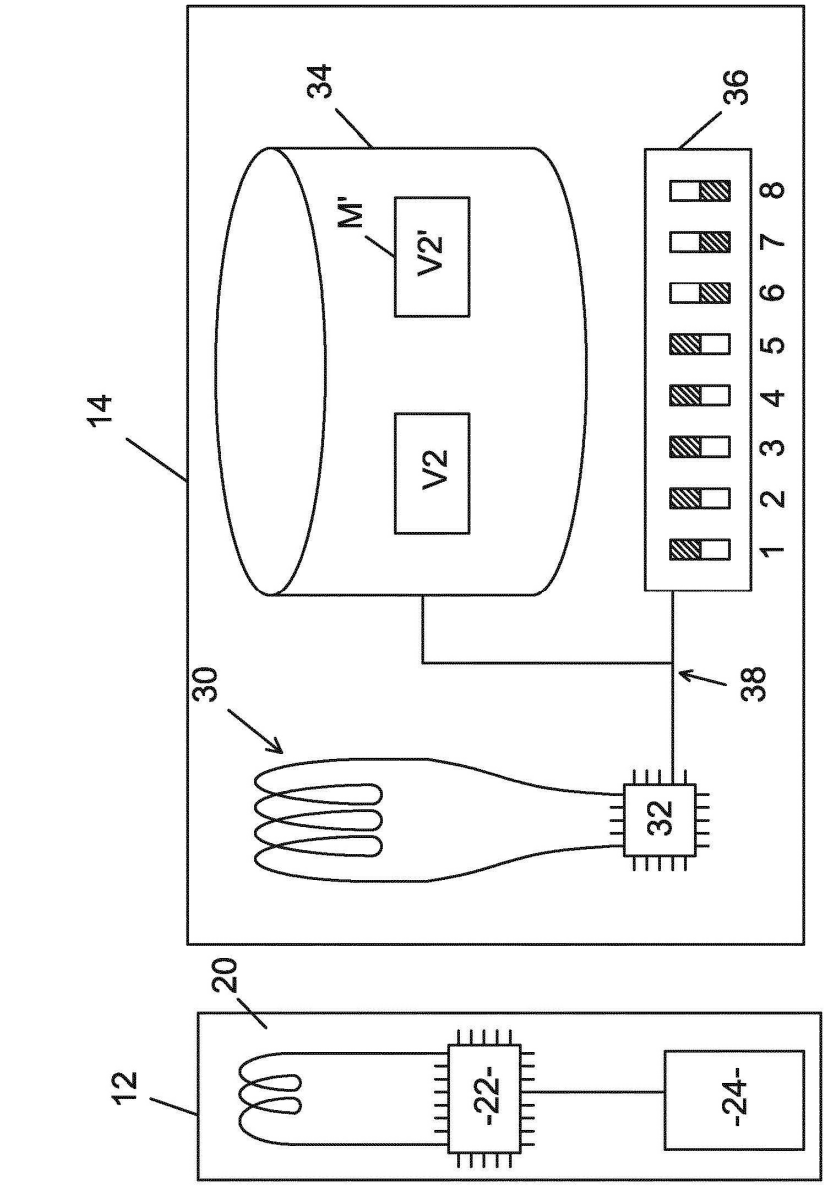

FIG.7

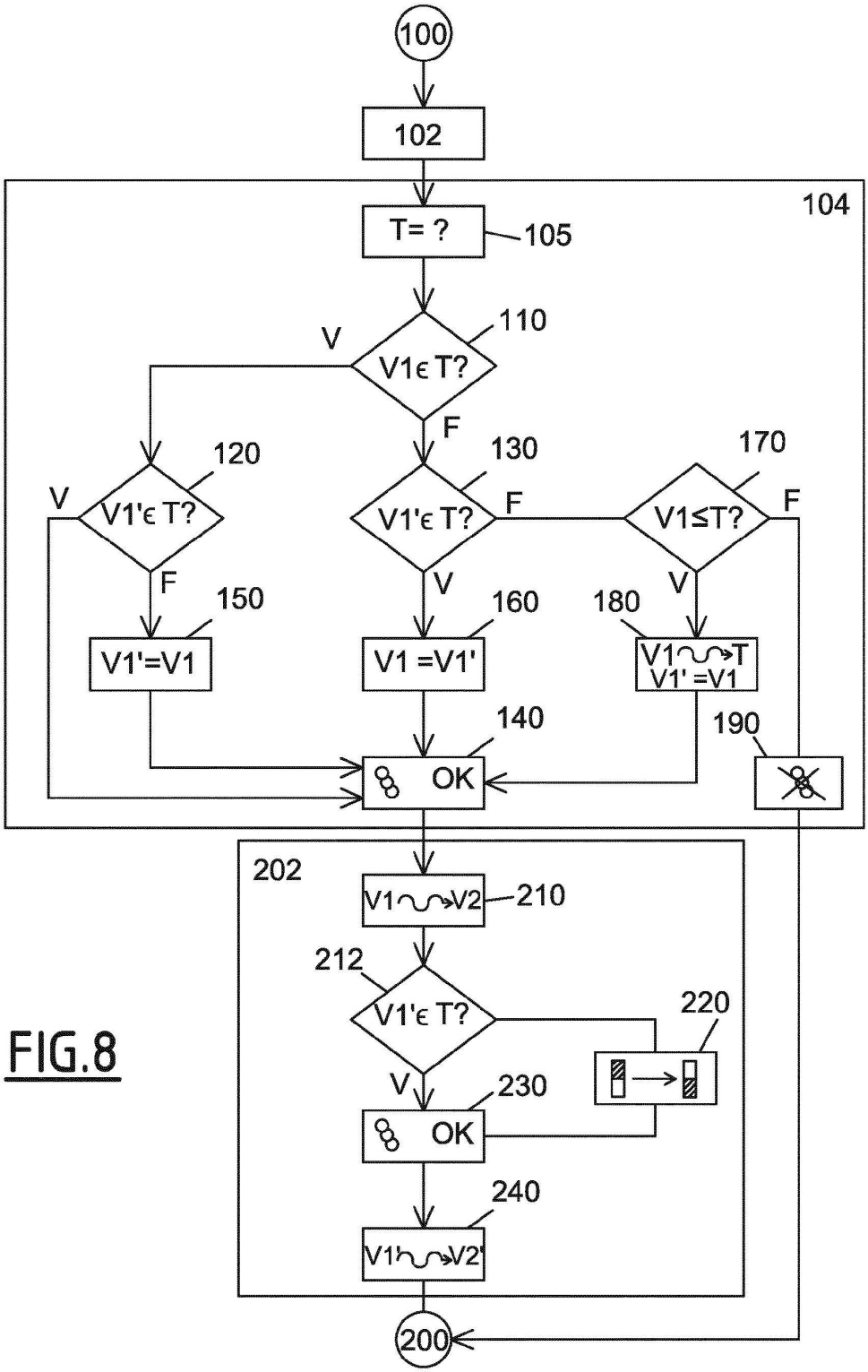
100
102
104
T= ?
105
110
V
V1ϵ T?
F
120
130
170
V
V1'ϵ T?
V1'ϵ T?
F
V1≤T?
F
F
V
V
150
160
180
V1'=V1
V1 =V1'
V1⇝T
V1' =V1
140
190
OK
202
V1⇝V2
210
212
V1'ϵ T?
220
V
230
OK
240
V1'⇝V2'
200

FIG.8