(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 556 681**

(21) Número de solicitud: 201430923

(51) Int. CI.:

G07C 13/00 (2006.01)

(12) SOLICITUD DE PATENTE A2

(22) Fecha de presentación:

17.06.2014

(43) Fecha de publicación de la solicitud:

19.01.2016

(71) Solicitantes:

BERMÚDEZ PÉREZ, Juan José (100.0%)
C/ Emigrant 30 Bajo 2
08906 L' Hospitalet de Llobregat (Barcelona) ES

(72) Inventor/es:

BERMÚDEZ PÉREZ, Juan José

(54) Título: **SISTEMA DE VOTO ELECTRÓNICO ANÓNIMO Y SEGURO EN REDES ABIERTAS**

(57) Resumen:
La presente invención tiene por objeto un método de voto electrónico del tipo que permite realizar votaciones sobre una cuestión desde terminales remotos interconectados mediante una red de comunicaciones abierta (por ejemplo Internet). El método se caracteriza por comprender (a) una fase en que se crean papeletas virtuales, (b) una fase en que se establece un orden entre los agentes votantes, (c) una fase en que cada Agente de Votación va extrayendo sucesivamente una papeleta virtual, (d) una fase en que el último agente hace públicas las papeletas restantes, (e) una fase en que cada agente verifica la coherencia de los datos y comunica cualquier posible error, (f) una fase en que cada agente pide información adicional al resto de agentes para hacer verificaciones de seguridad adicionales.

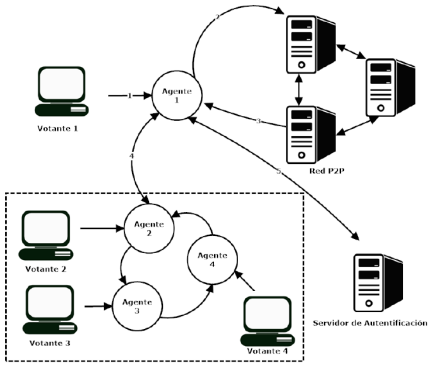

Figura 1a

ES 2 556 681 A2

DESCRIPCIÓN

Sistema de voto electrónico anónimo y seguro en redes abiertas

ANTECEDENTES

El estado de la técnica actual en lo que se refiere a sistemas de votación electrónica a través de una red de comunicaciones no segura (como pueda ser Internet) no ha conseguido hasta ahora eliminar la necesidad de que haya una o varias autoridades que supervisen el proceso electoral ni de que los participantes en dicha votación se vean obligados a depositar su confianza en que dichas autoridades (o elementos integrantes de las mismas) no se salten las normas en provecho propio. Sí se han resuelto problemas como el de evitar que el voto pueda ser manipulado o que cualquier otra persona pueda conocer el voto de un votante, pero generalmente mediante la implantación de infraestructuras muy caras, que necesitan además ser administradas por personal de confianza y ser auditadas por entidades independientes. En la práctica esto se traduce en que frecuentemente las elecciones organizadas por organismos públicos no permitan el voto a través de Internet.

El problema de garantizar el secreto de voto ha sido resuelto si se excluye de dicha garantía a la o las autoridades de confianza que recopilan los resultados de la votación o participan en alguna de las etapas del sistema de voto electrónico. Además, alguna invención consigue garantizar en teoría dicho secreto también respecto a dichas autoridades si se parte de la base de que éstas no cooperarán entre ellas para averiguar el voto de un ciudadano y de que no hay posibilidad de que elementos descontrolados dentro de las estructuras de dichas autoridades cooperen con dicho fin (WO 2003050771 A1, [Fujioka, A., Okamoto, T. y Ohta, K. A practical secret voting schemefor large scale elections. Proc. of Auscrypt '92, LNCS 718, pp. 244-251, 1992] , [Park, C, Itoh, K. y Kurosawa, K. Efficient anonymous channel and all/nothing election scheme. Proc. of Eurocrypt '93, LNCS 765, pp. 248-259, 1993], US 6,317,833). Algunas de dichas invenciones (por ejemplo WO 2003050771 A1) requieren además que haya varios programas informáticos de los que se garantice su correcto funcionamiento e imposibilidad de acceso no controlado. Un fallo de seguridad en el acceso a los mismos podría resultar catastrófico.

Definiciones:

Red P2P: Una red peer-to-peer, red de pares, red entre iguales, red entre pares o red punto a punto (P2P, por sus siglas en inglés) es una red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y servidores respecto a

los demás nodos de la red. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados.

BREVE DESCRIPCIÓN DE LA INVENCIÓN

La presente invención tiene por objeto un sistema de voto electrónico distribuido, anónimo y seguro.

El sistema consta de un terminal, entendiendo en la presente invención bajo el concepto de terminal cualquier dispositivo capaz de mostrar en unos medios de visualización el contenido de una página web o contenido digital, incluyendo en consecuencia ordenadores, móviles, ordenadores de mano, portátiles, relojes inteligentes, gafas inteligentes, televisiones digitales, etc. En caso de que el votante no fuese una persona sino un circuito electrónico o un computador, se puede omitir dicho terminal.

Un Agente de Votación (descargable o preinstalado en el terminal) que incorpora las operativas necesarias para que el voto del usuario sea procesado y contabilizado por el sistema. Dicho módulo incluye operativas de comunicación con otros terminales, operativas de encriptación y certificación de información y operativas de detección de errores o ataques maliciosos contra el proceso de elección. En caso de que el votante sea un circuito electrónico o computador, dicho Agente de Votación puede estar integrado en el mismo circuito, formar parte del software del computador, o formar parte de un dispositivo independiente conectado al circuito o computador.

Optativamente puede haber (a) un (o más) Servidor de Recuento central que recopila la información suministrada por los terminales, o (b) un conjunto de nodos interconectados mediante una r*ed P2P*, que recopilan la información, y la almacenan de forma distribuida y cooperativa.

Optativamente puede haber un (o más) Servidor de Autentificación de votantes (que puede coincidir con cualquier otro servidor de esta invención).

Optativamente puede haber un (o más) Servidor de Certificación (que puede coincidir con cualquier otro servidor de esta invención)

Optativamente puede haber un (o más) Servidor de Control de Clústeres (que puede coincidir con cualquier otro servidor de esta invención)

Optativamente puede haber un (o más) Servidor de Publicación de resultados (que puede coincidir con cualquiera de los servidores anteriores)

Las características de la invención hacen que, para garantizar el secreto y la inalterabilidad del voto, los votantes no deban depositar su confianza en la buena voluntad de una o varias

autoridades ni en los integrantes de las mismas. En algunas de las opciones de implantación de la presente invención intervienen autoridades de confianza que en teoría pueden tener un comportamiento indebido, pero con consecuencias menos graves que en invenciones anteriores. La información, incluso haciendo uso de servidores de autoridades de confianza, se encuentra siempre replicada y certificada contra modificaciones y resulta imposible para dichas autoridades conocer con certeza el voto individual de un votante. Cualquier comportamiento indebido que pretenda modificar el sentido del voto o la privacidad del voto, puede ser detectado por los votantes. En caso de acceso no autorizado a los servidores de alguna autoridad de confianza, cualquier alteración de los datos puede ser detectada y corregida simplemente recopilando de nuevo la información. En algunas de las opciones de implementación de la presente invención incluso no se requiere la existencia de autoridades de confianza que participen en el proceso de verificación de la votación.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La figura 1a representa un diagrama de bloques que ilustra un posible flujo de datos desarrollado durante la fase de conexión de la presente invención entre las partes que integran el sistema, cuando una de las partes integrantes es una *red P2P* que almacena los resultados de forma colaborativa. Corresponde a la fase 1 de la descripción en detalle de la invención:

- el Votante 1, por medio del Agente 1 (flecha 1), hace una petición de conexión (flecha 2) a la *red P2P*, la cual le responde (flecha 3) indicando los datos para conectarse a un clúster.

- El Agente 1 entonces hace la petición de conexión al clúster (flecha 4) y obtiene la lista de participantes en el clúster.

- El Agente 1 entonces verifica la identidad de los participantes por medio de un Servidor de Autentificación (flecha 5).

La figura 1b representa un diagrama de bloques que ilustra un posible flujo de datos desarrollado durante la fase de conexión de la presente invención entre las partes que integran el sistema, cuando hay una autoridad central que proporciona los datos de conexión a los clústeres de votación. Corresponde a la fase 1 de la descripción en detalle de la invención:

- el Votante 1, por medio del Agente 1 (flecha 1), hace una petición de conexión (flecha 2) al servidor de Control de Clústeres, el cual le responde (flecha 3) indicando los datos para conectarse a un clúster.

- El Agente 1 entonces hace la petición de conexión al clúster (flecha 4) y obtiene la lista de participantes en el clúster.

- El Agente 1 entonces verifica la identidad de los participantes por medio de un Servidor de Autentificación (flecha 5).

La figura 2 ilustra un caso de realización práctica en que el sistema de la invención es utilizado para contabilizar el voto de 4 usuarios, representando una simplificación del caso más general de utilización de la invención. Corresponde a la fase 2 de la descripción detallada de la invención:

- En la parte superior se muestra una tabla que describe la papeleta virtual que selecciona cada agente en cada ronda. Cada fila representa una ronda. La primera columna es el número de ronda. Las siguientes cuatro columnas son las elecciones realizadas por cada agente en cada ronda. La última columna muestra las papeletas restantes al final de cada ronda.

- En la parte inferior se muestra un grafo que describe paso a paso qué papeleta elige cada agente en cada momento. Dicha papeleta se muestra encima de cada círculo. Cada círculo representa una elección de un agente (el indicado en el interior del círculo). La entrada a cada círculo indica las papeletas que recibe el agente y la salida las papeletas restantes tras haber seleccionado la papeleta indicada. Cada agente repite esta operación 3 veces, tal como se describe en la tabla superior. La primera flecha de entrada contiene todas las papeletas generadas inicialmente y la última flecha de salida indica las papeletas virtuales que quedan al final del proceso. El valor de dichas papeletas permite deducir el resultado de la votación, tal como se describe en la explicación detallada.

La figura 3 muestra una tabla de verificación de la votación mostrada en la figura 2. Se ha implementado, para este ejemplo, un esquema de validación en que cada Agente pregunta al resto de Agentes de Votación un único identificador de opción de voto. Cada casilla de la tabla indica el valor que el agente de la columna pasa al agente de la fila. Esta figura ilustra los pasos dados en la fase 3 (verificación) de la descripción detallada de la presente invención.

Por ejemplo, la casilla correspondiente a columna Agente B, fila Agente A, tiene el identificador N3. Eso indica que el Agente A ha pedido al Agente B que le pase un identificador correspondiente a la opción N. El Agente B podía haber devuelto el identificador N3 o el N6, ya que en la primera ronda eligió el N3 y en la tercera el N6. El Agente A, cuando recibe el identificador N3 comprueba que dicho identificador no sea uno de los que él ha elegido ni uno de los que han quedado en la lista de papeleteas sobrantes.
En la casilla correspondiente a columna Agente C, fila Agente A, ahora el Agente A pide al

Agente C un identificador correspondiente a la opción R y éste devuelve el identificador R5 que había elegido en la tercera ronda.

EXPLICACIÓN DETALLADA DE LA INVENCIÓN

Notación:

Urna virtual: Elemento figurado que representa un contenedor del voto de varios votantes legítimos en una votación.

N: tamaño del clúster de una urna virtual

o: número de opciones que se puede votar

k: factor multiplicador

Los procesos y protocolos criptográficos que incluye la presente invención requieren la realización por parte del votante de cálculos matemáticos complejos La complejidad de estos cálculos motiva que sean realizados, en nombre del votante, por un Agente de Votación formado por un conjunto de programas o software

Supuestos previos:

- Cada votante dispone de un identificador único de la votación en que quiere participar y los datos de conexión a una lista de servidores proporcionados por una o varias autoridades de confianza.
- Cada votante dispone de un par de claves asimétricas otorgadas, o no, por una autoridad de confianza (habitualmente un organismo público). En España podría ser por ejemplo un certificado CERES o el DNI electrónico.
- Se ha establecido un censo que incluye las personas o entidades legitimadas a participar en la votación. Dicho censo puede haber sido realizado por una autoridad de confianza o por cualquier otro medio acordado por las partes involucradas en la votación.
- Opcionalmente, cada votante puede disponer de un identificador privado, proporcionado por una autoridad de confianza, que identifica al votante en la votación de forma única, pero que solo permite conocer la identidad real del votante a dicha autoridad de confianza.

Fase 1: Crear urna virtual.

Paso 1 (fig. 1a y 1b). El votante comunica al Agente de Votación su voto para una determinada elección en curso. Este paso no ha de realizarse obligatoriamente en primer lugar: puede

realizarse en cualquier momento antes de que el Agente de Votación extraiga ninguna papeleta virtual. Incluso podría implementarse de forma que el voto se elija con posterioridad sin que ello modifique el funcionamiento básico del proceso.

Paso 2 (fig. 1a y 1b). El Agente de Votación conecta a un Servidor de Control de Clústeres o a una *red P2P* y hace una solicitud de participación en la elección.

Paso 3 (fig. 1a y 1b). El Agente de Votación recibe los datos para conectarse a un clúster. Si no hay ninguno disponible se le comunica que ha de crear uno y esperar conexiones.

Paso 4 (fig. 1a y 1b). El Agente de Votación crea el clúster o se conecta al clúster indicado. Las comunicaciones entre los nodos del clúster se realizarán de forma segura por medio de cualquier protocolo disponible en el estado de la técnica o cualquier otro ideado expresamente para dicha comunicación. No forma parte de esta invención el protocolo seguro de comunicación entre los nodos.

Paso 5 (fig. 1a y 1b). El Agente de Votación verifica que los miembros del clúster estén legitimados para participar en la votación. Esta comprobación se puede hacer contra un Servidor de Autentificación de una autoridad de verificación o por cualquier otro medio. No forma parte de esta invención el protocolo de verificación de legitimidad para participar en la votación. El resto de miembros del clúster verifican a su vez la legitimidad del nuevo Agente para participar en la votación.

En el caso de usar una *red P2P* para almacenar de forma distribuida los resultados electorales, se podrá consultar igualmente si el usuario ya ha votado, o bien confiar en una autoridad verificadora, o bien confiar en la opinión de los nodos actualmente conectados a la *red P2P*, o bien saltarse esta verificación.

Si el clúster llega al número de Agentes conectados pactado (N) o a uno suficiente para iniciar la votación, y todos los agentes están de acuerdo en la legitimidad del clúster, se procede a la fase de votación.

Fase 2: Votación (figura 2)

Paso 1. El clúster crea un mínimo de N*(k+1) papeletas virtuales por cada opción de voto. Cada papeleta virtual tiene un identificador único asociado a la opción de voto que representa. Todos los agentes votantes en el clúster tienen la lista inicial de papeletas virtuales y conocen el voto que representa cada una. No forma parte de esta invención el protocolo para realizar

este paso. Se usará cualquier protocolo disponible en el estado de la técnica o cualquiera diseñado específicamente para este propósito.

Paso 2. Se establece un orden entre los agentes votantes (opcionalmente el orden se puede volver a establecer a cada vuelta del Bucle 1). No forma parte de esta invención el protocolo para establecer el orden entre los agentes votantes.

Hacer o*k+1 veces (Bucle 1):

Siguiendo el orden establecido, y hasta completar una vuelta completa a la lista de agentes, cada agente (Bucle 2):

Paso 3. Recibe del agente anterior de la lista, una lista de papeletas virtuales que quedan por elegir

Paso 4. Extrae una papeleta virtual de la lista y pasa el listado de papeletas restantes disponibles al siguiente en la lista (solo a él). El último de la lista, pasa la lista de papeletas virtuales restantes al primero de la lista.

Reglas que deben cumplir todos los agentes:

- Al finalizar las o*k+1 vueltas a la lista, cada agente debe tener al menos k papeletas correspondientes a cada opción de voto disponible, más una papeleta adicional que decanta su voto hacia la opción a que está asociada.
- Si se detecta alguna inconsistencia (por ejemplo que no queden papeletas de una opción), declarará inválida la urna virtual. Si un Agente declara inválida la urna virtual, el clúster se disuelve, y cada agente vuelve a buscar una urna virtual en la que incluirse. El voto de un solo agente puede disolver el clúster ya que el certificado no es válido si no está firmado por los N votantes.

Paso 5. El último agente en elegir anuncia al resto la lista de papeletas que han sobrado.

Paso 6. Cada Agente hace las comprobaciones pertinentes, como por ejemplo verificar que ninguna de las papeletas sobrantes corresponda a ninguna de las que ha elegido (significaría que algún agente ha alterado los datos).

Fase 3 Validación (figura 3)

Paso 1. Cada Agente pide a una serie de Agentes un (o más) identificador de papeleta virtual asociado a una determinada opción de voto. Éstos responden de forma privada al Agente que pregunta (ningún otro nodo del clúster conoce la respuesta). El Agente que pregunta verifica que no haya datos incoherentes. Se puede elegir cualquier algoritmo para seleccionar qué Agentes preguntan, a quién preguntan, cuántas opciones de voto preguntan a cada Agente,

cómo eligen la (o las) opción de voto de la que se debe presentar papeleta virtual para cada Agente al que preguntan, y cómo determinan si los datos son incoherentes. Una posible realización sería que 20 agentes elegidos al azar preguntan al resto de agentes aleatoriamente por una opción, y se detecta una incoherencia si alguien repite un identificador de papeleta virtual o el identificador de la papeleta virtual está en la lista de identificadores sobrantes tras la votación. Si se detecta alguna incoherencia se invalida toda la votación. El objetivo es que la probabilidad de que alguien haga trampa y no sea detectado sea muy pequeña y que al mismo tiempo la probabilidad de que algún agente votante averigüe el voto de algún otro agente sea nula o muy pequeña. No forma parte de esta invención ningún protocolo concreto para realizar este paso sino solo las características generales, explicitadas en este punto, que deberá tener dicho protocolo.

Paso 2. Si todos los agentes están de acuerdo en que no ha habido ningún error se genera un certificado digital firmado con la clave privada de cada votante. El certificado incluye (al menos) el resultado de la votación, el cual se deduce de las papeletas que han sobrado, y un identificador de cada votante. El identificador asociado a cada votante puede ser público (permite a cualquiera conocer la identidad del votante) o conocido únicamente por una autoridad de confianza coordinada con la autoridad de confianza encargada del recuento de votos (pueden ser ambas la misma).

Fase 4: Certificación de votación

Paso 1 (opcional)

Se envía el certificado a un (o más) Servidor de Certificación, el cuál firma el certificado con su clave privada y lo devuelve a cada uno de los Agentes de Votación para que estos sustituyan el certificado original por el firmado por la autoridad. Opcionalmente dicho Servidor de Certificación puede verificar diferentes parámetros de la votación, como pueda ser que no se haya superado el número de votos permitidos por votante.

Paso 2.

Se entrega el certificado a una autoridad de confianza encargada del recuento o a la *red P2P*.

Si se entrega a una autoridad de confianza (a través de servidor de Recuento), ésta lo almacena hasta finalizar la elección. Opcionalmente dicho Servidor de Recuento podría verificar diferentes parámetros de la votación, como pueda ser que no se haya superado el número de votos permitidos por votante. Opcionalmente, cada Agente podrá entregar el resultado a más autoridades de confianza o entidades independientes que supervisen el proceso.

Si se entrega a una *red P2P*, los nodos de dicha red retransmiten el certificado a toda la red de acuerdo al algoritmo colaborativo que utilicen. Una vez el certificado se ha incorporado a la *red P2P*, cualquiera puede obtener los datos de ésta para verificar la votación.

Fase 5: Recuento y consulta de resultados de la elección

Una vez finalizado el periodo de votación:

Si se ha establecido una autoridad de confianza para el recuento, ésta suma los resultados de todas las urnas virtuales. La suma corresponde al resultado general de la elección. A continuación transmite al Servidor de Publicación el resultado, y una lista con el identificador de cada urna virtual y el resultado de la votación en dicha urna, para que todos los usuarios puedan verificar que se ha contabilizado su voto y ver los resultados. Opcionalmente puede publicarse también el identificador (público o privado) de cada votante.

Si se ha usado una *red P2P*, ésta almacena la lista de resultados en cada urna virtual. Cualquier usuario puede sumar los resultados parciales y comprobar cuál es el resultado de la votación, así como comprobar que su voto está incluido. Opcionalmente puede haber Servidores de Publicación que recopilan dicha información y los votantes pueden consultar de dichos servidores el resultado.

En una de las variantes de implementación, la *red P2P* almacena los resultados de la votación encriptados mediante una clave generada por una autoridad central, y al finalizar el proceso electoral, dicha autoridad hace pública la clave que permite descifrar los datos. De esta manera no se conocen los resultados parciales de la votación hasta que ésta no ha concluido, y por lo tanto se evita que los resultados parciales puedan influir a algunos votantes. No forma parte de esta invención el protocolo para encriptar los votos. Una posible implementación de dicho protocolo consistiría en usar un par de claves asimétricas. La clave pública serviría para codificar el resultado de las Urnas Virtuales y la clave privada se haría pública al finalizar la votación.

REIVINDICACIONES

1- Método para votación electrónica segura, en el que se utiliza al menos un Servidor de Control de Clústeres y un conjunto de Agentes de Votación , estando dotados cada uno de ellos de medios de computación y preferiblemente conectados entre sí, en caso de dispersión, mediante al menos una red de comunicaciones, comprendiendo unos procesos y protocolos criptográficos para que a lo largo de la ejecución del método y una vez finalizado un proceso electoral, se garanticen una serie de requisitos de seguridad específicos del proceso electoral, caracterizado por comprender las siguientes etapas: a) creación de una Urna Virtual formada por diversos Agentes de Votación que verifican mutuamente la legitimidad para votar de cada votante ; b) intercambio de mensajes entre los Agentes de Votación siguiendo los siguientes pasos:

(i) Crear papeletas virtuales

(ii) Se establece un orden entre los agentes votantes

(iii) Hacer o*k+1 veces: Siguiendo el orden establecido, y hasta completar una vuelta completa a la lista de agentes, cada agente: (iv) recibe del agente anterior de la lista, una lista de papeletas virtuales que quedan por elegir, y (v) extrae una papeleta virtual de la lista y pasa el listado de papeletas restantes al siguiente agente. Dicha elección de papeleta deberá respetar la norma de que al final del proceso (o*k+1 elecciones) cada agente deberá haber elegido k papeletas de cada opción más una papeleta adicional que identifica la opción que han votado.

(vi) El último agente en elegir anuncia al resto la lista de papeletas que han sobrado.

(vii) Cada Agente de Votación hace las comprobaciones pertinentes para verificar la coherencia de los datos

c) Cada Agente de Votación pide a una serie de Agentes de Votación un (o más) identificador de papeleta virtual asociado a una determinada opción de voto. Estos responden de forma privada al Agente de Votación que pregunta (ningún otro nodo del clúster conoce la respuesta). El Agente de Votación que pregunta verifica que no haya datos incoherentes en la respuesta.

d) Opcionalmente, los Agentes de Votación firman el resultado.

2- Método, según la reivindicación 1, caracterizado porque los Agentes de Votación, al terminar la fase de verificación, comunican a uno o más Servidores de Recuento el resultado de la votación, el cuál almacena los resultados de las Urnas Virtuales y puede bien (a) usarlos para calcular el resultado y enviarlo a uno o más Servidores de Publicación (el mismo Servidor de Recuento puede hacer a su vez de Servidor de Publicación); o (b) retransmitir dichos resultados a otros Servidores de Recuento.

3- Método, según la reivindicación 1, caracterizado porque los Agentes de Votación, al terminar la fase de verificación, comunican a una *red P2P* el resultado de la votación, la cuál almacena los resultados de las Urnas Virtuales en una estructura de datos distribuida y puede bien (a) usarlos para calcular el resultado y enviarlo a uno o más Servidores de Publicación o (b) retransmitir dichos resultados a otros Servidores de Recuento, o (c) permitir a cualquiera descargar los resultados y calcular el resultado.

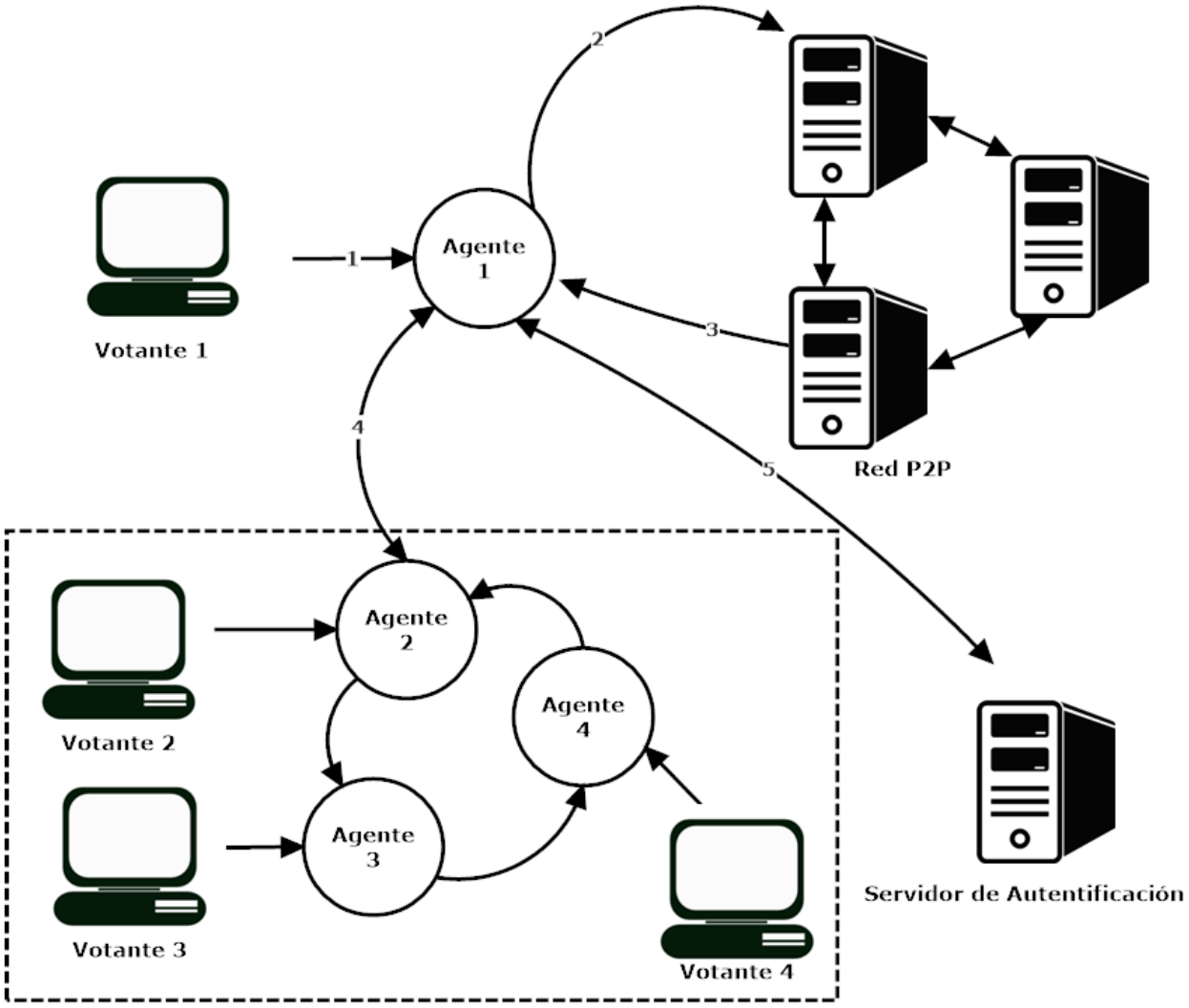
2
Votante 1
1
Agente 1
3
4
5
Red P2P
Agente 2
Votante 2
Agente 4
Agente 3
Votante 3
Votante 4
Servidor de Autentificación

Figura 1a

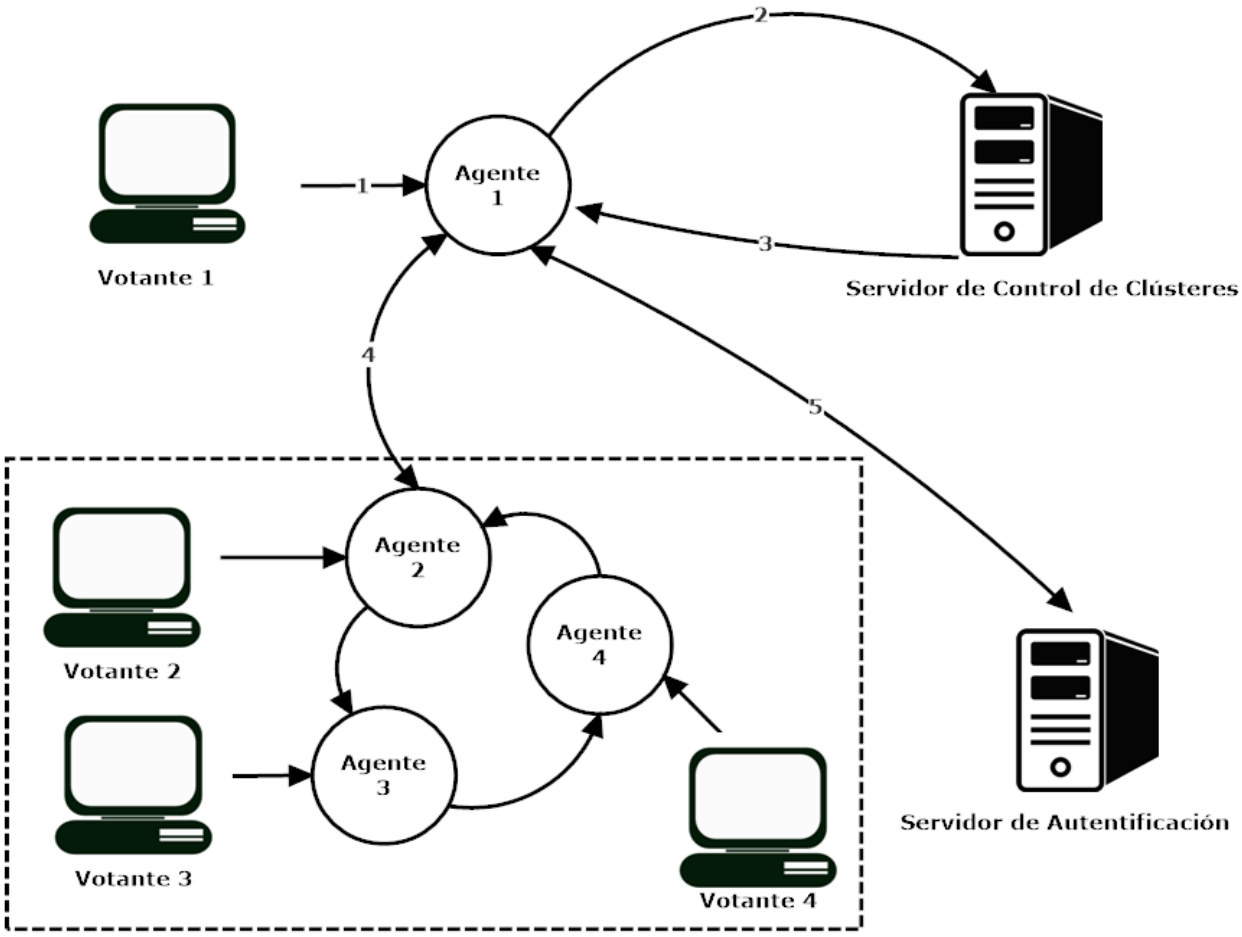
2
Agente 1
1
Votante 1
3
Servidor de Control de Clústeres
4
5
Agente 2
Agente 4
Votante 2
Agente 3
Votante 3
Votante 4
Servidor de Autentificación

Figura 1b

	Agente A	Agente B	Agente C	Agente D	Papeletas virtuales restantes
Ronda 1	N1	N3	N2	R1	N4,N5,N6,N7,N8,R2,R3,R4,R5,R6,R7,R8
Ronda 2	N8	R3	N4	R2	N5,N6,N7,R4,R5,R6,R7,R8
Ronda 3	R4	N6	R5	N7	N5,R6,R7,R8

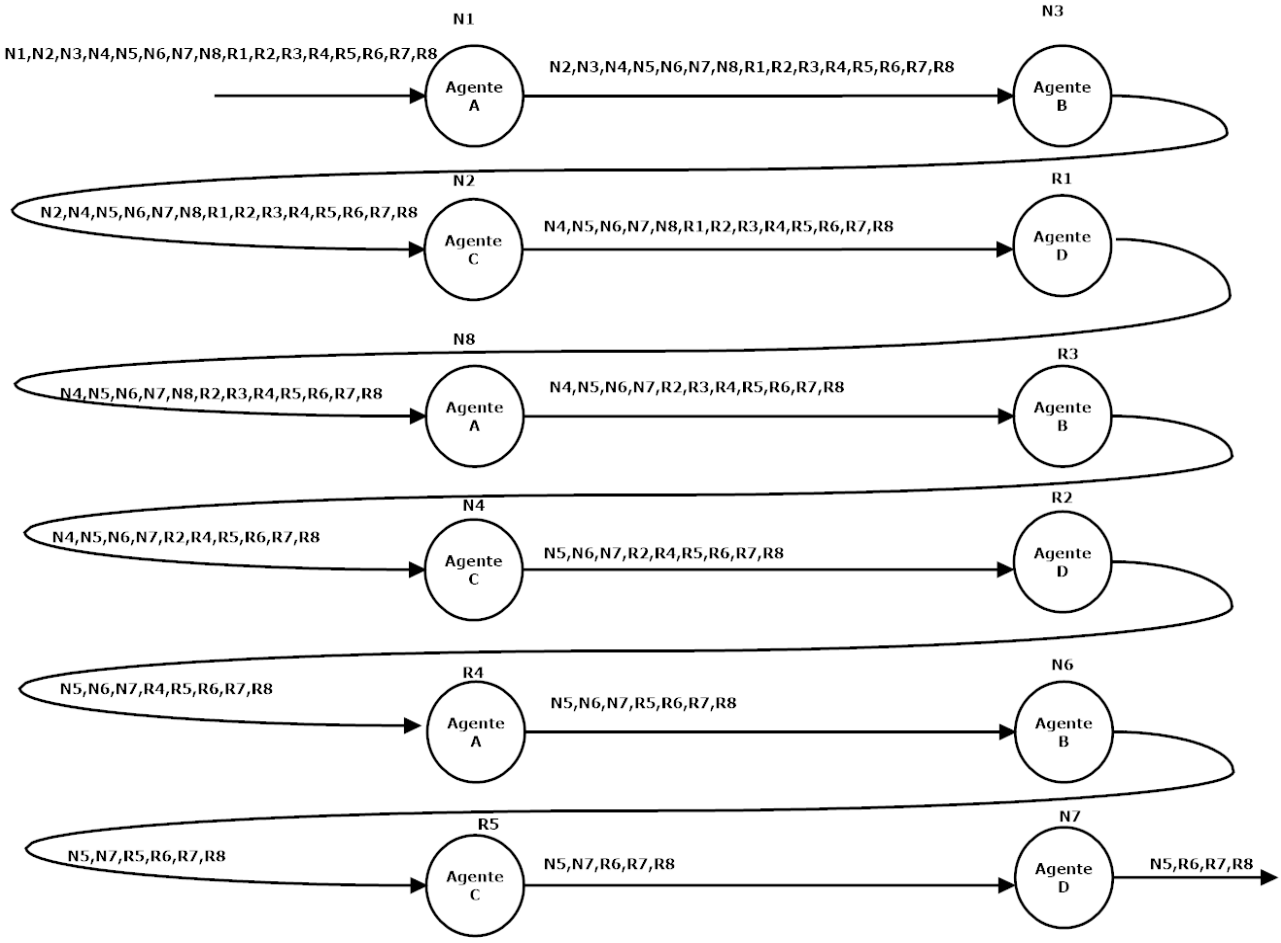

Figura 2

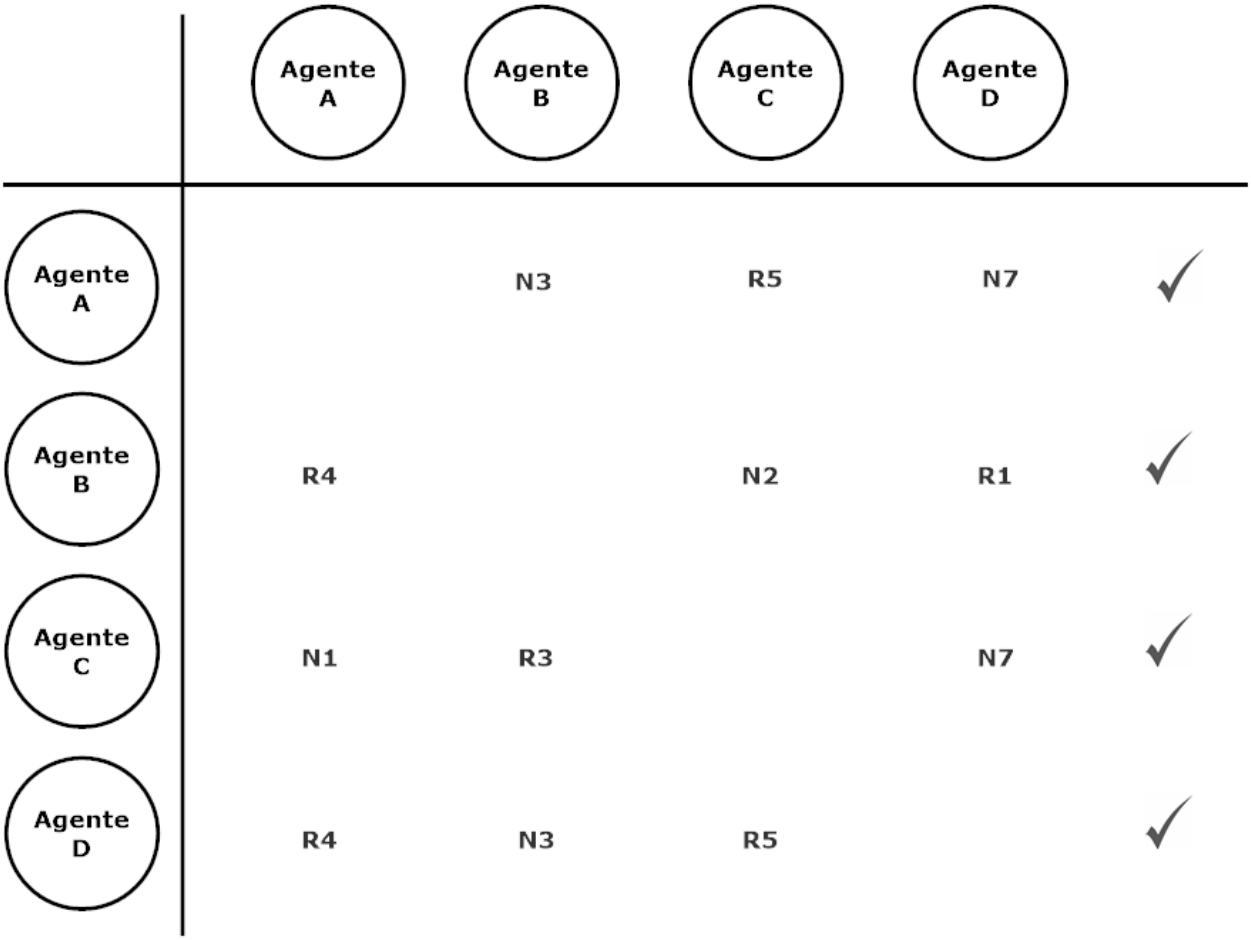
Agente A
Agente B
Agente C
Agente D
Agente A
N3
R5
N7
Agente B
R4
N2
R1
Agente C
N1
R3
N7
Agente D
R4
N3
R5

Figura 3